Service-Authorization-Referenz

Service-Authorization-Referenz

Service-Authorization-Referenz: Service-Authorization-Referenz

Table of Contents

Referenz

Die Service-Autorisierungsreferenz enthält eine Liste der Aktionen, Ressourcen und Bedingungsschlüssel, die von jedem AWS-Service unterstützt werden. Sie können Aktionen, Ressourcen und Bedingungsschlüssel in AWS Identity and Access Management(IAM)-Richtlinien angeben, um den Zugriff auf AWS-Ressourcen zu verwalten.

Inhalt

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Dienste

Jeder AWS Dienst kann Aktionen, Ressourcen und Bedingungskontextschlüssel für die Verwendung in IAM-Richtlinien definieren. In diesem Thema wird beschrieben, wie die für die einzelnen Services bereitgestellten Elemente dokumentiert sind.

Jedes Thema besteht aus Tabellen mit Listen der verfügbaren Aktionen, Ressourcen und Bedingungsschlüssel.

Die Tabelle der Aktionen

Die Tabelle Actions (Aktionen) listet alle Aktionen auf, die Sie im Element `Action` einer IAM-Richtlinienanweisung verwenden können. Nicht alle API-Produktionen, die von einem Service definiert werden, können in einer IAM-Richtlinie als Aktion verwendet werden. Einige Services enthalten „nur mit Berechtigung“-Aktionen, die nicht direkt einer API-Operation entsprechen. Diese Aktionen sind mit [nur mit Genehmigung] gekennzeichnet. Verwenden Sie diese Liste, um zu ermitteln, welche Aktionen Sie in einer IAM-Richtlinie verwenden können. Weitere Informationen zu den Elementen `Action`, `Resource` oder `Condition` finden Sie unter IAM-JSON-Richtlinienelementreferenz. Die Tabellenspalten Actions (Aktionen) und Description (Beschreibung) sind selbsterklärend.

- Die Spalte Zugriffsebene gibt an, wie die Aktion klassifiziert ist (Auflisten, Lesen, Schreiben, Berechtigungsverwaltung oder Tagging). Diese Klassifizierung gibt an, welche Zugriffsebene die betreffende Aktion gewährt, wenn Sie sie in einer Richtlinie verwenden. Weitere Informationen über Zugriffsebenen finden Sie unter Übersicht auf Zugriffsebene innerhalb von Richtlinienübersichten.

- Die Spalte Ressourcentypen gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn die Spalte leer ist, unterstützt die Aktion keine Berechtigungen auf Ressourcenebene und Sie müssen alle Ressourcen („*“) in Ihrer Richtlinie angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie den Ressourcen-ARN im Element `Resource` Ihrer Richtlinie angeben. Weitere Informationen zu dieser Ressource finden Sie in der entsprechenden Zeile der Tabelle Ressourcentypen. Alle Aktionen und Ressourcen, die in einer einzelnen Anweisung enthalten sind, müssen miteinander kompatibel sein. Wenn Sie eine Ressource angeben, die für die Aktion nicht gültig ist, schlägt eine Anforderung zum Verwenden der Aktion fehl und das Element `Effect` der Anweisung wird nicht angewendet.

  Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie einen Berechtigungs-ARN auf Ressourcenebene in einer Anweisung mit dieser Aktion angeben, muss er von diesem Typ sein. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen Typ entscheiden.
- Die Spalte Bedingungsschlüssel enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Bedingungsschlüssel können mit einer Aktion oder mit einer Aktion und einer bestimmten Ressource unterstützt werden. Achten Sie genau darauf, ob sich der Schlüssel in derselben Zeile wie ein bestimmter Ressourcentyp befindet. Diese Tabelle enthält keine globalen Bedingungsschlüssel, die für Aktionen oder unter nicht damit im Zusammenhang stehenden Umständen verfügbar sind. Weitere Informationen über globale Bedingungsschlüssel finden Sie unter Globale AWS -Bedingungskontextschlüssel.
- Die Spalte Abhängige Aktionen gibt alle Berechtigungen an, die Sie zusätzlich zur Berechtigung für die Aktion selbst benötigen, damit die Aktion erfolgreich aufgerufen werden kann. Dies kann erforderlich sein, wenn die Aktion auf mehr als eine Ressource zugreift.

  Abhängige Aktionen sind nicht in allen Szenarien erforderlich. Weitere Informationen zur Bereitstellung detaillierter Berechtigungen für Benutzer finden Sie in der Dokumentation des jeweiligen Services.

Die Tabelle der Ressourcentypen

Die Tabelle Ressourcentypen listet alle Ressourcentypen auf, die Sie als ARN im `Resource`-Richtlinienelement angeben können. Nicht jeder Ressourcentyp kann mit jeder Aktion angegeben werden. Einige Ressourcentypen funktionieren nur mit bestimmten Aktionen. Wenn Sie einen Ressourcentyp in einer Anweisung mit einer Aktion angeben, die diesen Ressourcentyp nicht

unterstützt, erlaubt die Anweisung keinen Zugriff. Weitere Informationen zum Element `Resource` finden Sie unter IAM-JSON-Richtlinienelemente: Resource.

- Die Spalte ARN gibt das Amazon-Ressourcennamen (ARN)-Format an, mit dem auf Ressourcen dieses Typs verwiesen werden muss. Die Bestandteile mit vorangestelltem $ müssen durch die tatsächlichen Werte für das jeweilige Szenario ersetzt werden. Beispiel: Wenn in einem ARN `$user-name` steht, müssen Sie diese Zeichenfolge durch den tatsächlichen Namen eines Benutzers oder eine Richtlinienvariable ersetzen, die den Namen eines Benutzers enthält. Weitere Informationen zu ARNs finden Sie unter IAM-ARNs.
- Die Spalte Bedingungsschlüssel gibt Bedingungskontextschlüssel an, die Sie in eine IAM-Richtlinienanweisung nur dann einfügen können, wenn sowohl diese Ressource als auch eine unterstützende Aktion aus der Tabelle oben in der Anweisung enthalten sind.

Die Tabelle der Bedingungsschlüssel

Die Tabelle Bedingungsschlüssel listet alle Bedingungskontextschlüssel auf, die Sie im Element `Condition` einer IAM-Richtlinienanweisung verwenden können. Nicht jeder Schlüssel kann mit jeder Aktion oder Ressource angegeben werden. Bestimmte Schlüssel funktionieren nur mit bestimmten Aktions- und Ressourcentypen. Weitere Informationen zum Element `Condition` finden Sie unter IAM-JSON-Richtlinienelemente: Condition.

- Die Spalte Type (Typ) gibt den Datentyp des Bedingungsschlüssels an. Dieser Datentyp bestimmt, welche Bedingungsoperatoren Sie zum Vergleichen von Werten in der Anforderung mit den Werten in der Richtlinienanweisung verwenden können. Sie müssen einen Operator verwenden, der für den Datentyp geeignet ist. Wenn Sie einen falschen Operator verwenden, wird nie eine Übereinstimmung ermittelt und die Richtlinienanweisung nie angewendet.

  Wenn die Spalte Type (Typ) eine Liste eines der einfachen Typen angibt, können Sie mehrere Schlüssel und Werte in Ihren Richtlinien verwenden. Verwenden Sie dazu Bedingungssatzpräfixe mit Ihren Operatoren. Verwenden Sie das Präfix `ForAllValues`, um anzugeben, dass alle Werte in der Anforderung mit einem Wert in der Richtlinienanweisung übereinstimmen müssen. Verwenden Sie das Präfix `ForAnyValue`, um anzugeben, dass mindestens ein Wert in der Anforderung mit einem der Werte in der Richtlinienanweisung übereinstimmen muss.

Themen

- Aktionen, Ressourcen und Bedingungsschlüssel für AWS-Kontenverwaltung

- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Activate
- Aktionen, Ressourcen und Bedingungsschlüssel für Alexa for Business
- Aktionen, Ressourcen und Bedingungsschlüssel für AmazonMediaImport
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Amplify
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Amplify Admin
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Amplify UI Builder
- Aktionen, Ressourcen und Bedingungsschlüssel für Apache-Kafka-APIs für Amazon-MSK-Cluster
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon API Gateway
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon-API-Gateway-Management
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon-API-Gateway-Management V2
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS App Mesh
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS App Mesh Preview
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS App Runner
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS-App2Container
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS AppConfig
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS AppFabric
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon AppFlow
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon AppIntegrations
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Application Auto Scaling
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS-Application-Cost-Profiler-Service
- Aktionen, Ressourcen und Bedingungsschlüssel für Application Discovery Arsenal
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Application Discovery Service
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Application Migration Service
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Application Transformation Service
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon AppStream 2.0
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS AppSync
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Artifact
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Athena
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Audit Manager

- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Auto Scaling
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS B2B Data Interchange
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Backup
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Backup Gateway
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Backup-Speicher
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Batch
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Bedrock
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Billing
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Billing und Datenexporte für das Kostenmanagement
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Billing Conductor
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Billing-Konsole
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Braket
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Budget Service
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS BugBust
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Certificate Manager
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Chatbot
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Chime
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Clean Rooms
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Clean Rooms ML
- Aktionen, Ressourcen und Bedingungsschlüssel für die AWS Cloud Control API
- Aktionen, Ressourcen und Bedingungskontextschlüssel für Amazon Cloud Directory
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Cloud Map
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Cloud9
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS CloudFormation
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CloudFront
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CloudFront Schlüsselwertspeicher
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS CloudHSM
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CloudSearch

- Aktionen, Ressourcen und Bedingungsschlüssel für AWS CloudShell
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS CloudTrail
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS-CloudTrail-Daten
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CloudWatch
- Aktionen, Ressourcen und Zustandsschlüssel für Amazon CloudWatch Application Insights
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CloudWatch Evidently
- Aktionen, Ressourcen und Zustandstasten für Amazon CloudWatch Internet Monitor
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CloudWatch Logs
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CloudWatch Network Monitor
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CloudWatch Observability Access Manager
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS CloudWatch RUM
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CloudWatch Synthetics
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS CodeArtifact
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS CodeBuild
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CodeCatalyst
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS CodeCommit
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS CodeConnections
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS CodeDeploy
- Aktionen, Ressourcen und Bedingungsschlüssel für sichere Host-Befehle mit dem AWS-CodeDeploy-Service
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CodeGuru
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CodeGuru Profiler
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CodeGuru Reviewer
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CodeGuru Security
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS CodePipeline
- Aktionen, Ressourcen und Zustandsschlüssel für AWS CodeStar
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS CodeStar Connections
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS CodeStar Notifications
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CodeWhisperer

- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Cognito Identity
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Cognito Sync
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Cognito-Benutzerpools
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Comprehend
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Comprehend Medical
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Compute Optimizer
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Config
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Connect
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Connect Cases
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Connect Customer Profiles
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Connect Voice ID
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Connector Service
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Management Console Mobile App
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Consolidated Billing
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Control Catalog
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Control Tower
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Kosten- und Nutzungsbericht
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Cost Explorer Service
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Cost Optimization Hub
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Customer Verification Service
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Data Exchange
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Data Lifecycle Manager
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Data Pipeline
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Database Migration Service
- Aktionen, Ressourcen und Bedingungsschlüssel für Database Query Metadata Service
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS DataSync
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon DataZone
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Deadline Cloud
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS DeepComposer

- Aktionen, Ressourcen und Bedingungsschlüssel für AWS DeepLens
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS DeepRacer
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Detective
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Device Farm
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon DevOps Guru
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Diagnosetools
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Direct Connect
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Directory Service
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon DocumentDB Elastic Clusters
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon DynamoDB
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon DynamoDB Accelerator (DAX)
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2 Auto Scaling
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2 Image Builder
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2 Instance Connect
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EKS Auth
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elastic Beanstalk
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Elastic Block Store
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Elastic Container Registry
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Elastic Container Registry Public
- Aktionen, Ressourcen und Bedingungsschlüssel für den Amazon Elastic Container Service
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elastic Disaster Recovery
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Elastic File System
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Elastic Inference
- Aktionen, Ressourcen und Bedingungsschlüssel für den Amazon Elastic Kubernetes Service
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elastic Load Balancing
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elastic Load Balancing V2
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Elastic MapReduce
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Elastic Transcoder

- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon ElastiCache
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elemental Appliances and Software
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elemental Appliances and Software Activation Service
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elemental MediaConnect
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elemental MediaConvert
- Aktionen, Ressourcen und Zustandstasten für AWS Elemental MediaLive
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elemental MediaPackage
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elemental MediaPackage V2
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elemental MediaPackage VOD
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elemental MediaStore
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elemental MediaTailor
- Aktionen, Ressourcen und Bedingungsschlüssel für elementare Supportfälle für AWS
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elemental Support Content
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EMR in EKS (EMR-Container)
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EMR Serverless
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Entity Resolution
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EventBridge
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EventBridge Pipes
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EventBridge Scheduler
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EventBridge Schemas
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Fault Injection Service
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon FinSpace
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon FinSpace-API
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Firewall Manager
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Forecast
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Fraud Detector
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Free Tier
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon FreeRTOS

- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon FSx
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon GameLift
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Global Accelerator
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Glue
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Glue DataBrew
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Ground Station.
- Aktionen, Ressourcen und Zustandsschlüssel für Amazon GroundTruth Labeling
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon GuardDuty
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Health-APIs und -Benachrichtigungen
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS HealthImaging
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS HealthLake
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS HealthOmics
- Aktionen, Ressourcen und Bedingungsschlüssel für ausgehende Kommunikation mit hohem Volumen
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Honeycode
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS IAM Access Analyzer
- Aktionen, Ressourcen und Zustandsschlüssel für AWS IAM Identity Center (Nachfolger von AWS Single Sign-On)
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS IAM Identity Center (Nachfolger von AWS Single Sign-On)-Directory
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS IAM Identity Center OIDC-Service
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Identity and Access Management (IAM)
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Identity And Access Management
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Identity Store
- Aktionen, Ressourcen und Bedingungsschlüssel Identitätsspeicher-Authentifizierung für AWS
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS die Identitätssynchronisierung
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Import Export Disk Service
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Inspector
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Inspector2
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon InspectorScan

- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Interactive Video Service
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Interactive Video Service Chat.
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Invoicing Service
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT 1-Click
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT Analytics
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT Core Device Advisor
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT Device Tester
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT Events
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT Fleet Hub for Device Management
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT FleetWise
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT Greengrass
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT Greengrass V2
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT Jobs DataPlane
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT RoboRunner
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT SiteWise
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT TwinMaker
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT Wireless
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS IQ
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS IQ Berechtigungen
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Kendra
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Kendra Intelligent Ranking
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Key Management Service
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Keyspaces (für Apache Cassandra)
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Kinesis Analytics
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Kinesis Analytics V2
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Kinesis Data Streams
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Kinesis Firehose
- Aktionen, Ressourcen und Bedingungskontextschlüssel für Amazon Kinesis Video Streams

- Aktionen, Ressourcen und Zustandsschlüssel für AWS Lake Formation
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS-Lambda
- Aktionen, Ressourcen und Bedingungsschlüssel für den AWS Launch Wizard
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Lex
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Lex V2
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS License Manager
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS License Manager Linux Subscriptions Manager
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS License Manager User Subscriptions
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Lightsail
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Location
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Lookout for Equipment
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Lookout for Metrics
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Lookout for Vision
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Machine Learning
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Macie
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS -Mainframe-Modernisierungsservice
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Managed Blockchain
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Managed Blockchain Query
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Managed Grafana
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Managed Service for Prometheus
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Managed Streaming for Apache Kafka
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Managed Streaming for Kafka Connect
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Managed Workflows for Apache Airflow
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace -Katalog
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace Commerce Analytics Service

- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace Deployment Service
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace Discovery
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace Entitlement Service
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace Image Building Service
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace Management Portal
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace Metering Service
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace Private Marketplace
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace Procurement Systems Integration
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace Seller Reporting
- Aktionen, Ressourcen und Zustandsschlüssel für AWS Marketplace Anbietereinblicke
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Mechanical Turk
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Mobile Analytics
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Message Delivery Service
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Message Gateway Service
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Microservice Extractor für .NET
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS-Guthaben für das Programm zur Migrationsbeschleunigung
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Migration Hub
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Migration Hub Orchestrator
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Migration Hub Refactor Spaces
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Migration Hub Strategy Recommendations
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Mobile Analytics
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Monitron
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon MQ
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Neptune
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Neptune Analytics
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Network Firewall
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Network Manager

- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Network Manager Chat
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Nimble Studio
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon One Enterprise
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon OpenSearch Ingestion
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon OpenSearch Serverless
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon OpenSearch Service
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS OpsWorks
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS OpsWorks Configuration Management
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Organizations
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Outposts
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Panorama
- Aktionen, Ressourcen und Bedingungsschlüssel für die zentrale AWS-Parnter-Kontoverwaltung
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Payment Cryptography
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Payments
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Performance Insights
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Personalize
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Pinpoint
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Pinpoint Email Service
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Pinpoint SMS and Voice Service
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Pinpoint SMS Voice V2
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Polly
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Price List
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Private CA Connector for Active Directory
- Aktionen, Ressourcen und Bedingungsschlüssel für die private Zertifizierungsstelle für AWS
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Proton
- Aktionen, Ressourcen und Zustandsschlüssel für AWS Purchase Orders Console
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Q
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Q Business
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Q Business Q Apps

- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Q in Connect
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon QLDB
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon QuickSight
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon RDS
- Aktionen, Ressourcen und Bedingungsschlüssel für die Amazon RDS-Daten-API
- Aktionen, Ressourcen und Bedingungsschlüssel für die Amazon RDS-IAM-Authentifizierung
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS re:Post Private
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Recycle Bin
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Redshift
- Aktionen, Ressourcen und Bedingungsschlüssel für die Amazon Redshift-Daten-API
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Redshift Serverless
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Rekognition
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Resilience Hub
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Resource Access Manager (RAM)
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Resource Explorer
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Resource Group Tagging API
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Resource Groups
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon RHEL Knowledgebase Portal
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS RoboMaker
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Route 53
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Route 53 Recovery Controller – Zonal Shift
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Route 53 Domains
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Route 53 53-Profile ermöglichen die gemeinsame Nutzung von DNS-Einstellungen mit VPCs
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Route 53 Recovery Cluster
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Route 53 Recovery Controls
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Route 53 Recovery Readiness
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Route 53 Resolver
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon S3

- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon S3 Express
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon S3 Glacier
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon S3 Object Lambda
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon S3 in Outposts
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon SageMaker
- Aktionen, Ressourcen und Bedingungsschlüssel für Geodatenfunktionen von Amazon SageMaker
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon SageMaker Ground Truth Synthetic
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Savings Plans
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Secrets Manager
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Security Hub
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Security Lake
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Security Token Service
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Server Migration Service
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Serverless Application Repository
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Service Catalog
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS-Service, der verwaltete private Netzwerke bereitstellt
- Aktionen, Ressourcen und Bedingungsschlüssel für Service Quotas
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon SES
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Shield
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Signer
- Aktionen, Ressourcen und Bedingungstasten für AWS Signin
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Simple Email Service v2
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Simple Workflow Service
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon SimpleDB
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS SimSpace Weaver
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Snow Device Management
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Snowball
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon SNS
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS SQL Workbench

- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon SQS
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Step Functions
- Aktionen, Ressourcen und Zustandsschlüssel für AWS Storage Gateway
- Aktionen, Ressourcen und Bedingungsschlüssel für die AWS -Lieferkette
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Support
- Aktionen, Ressourcen und Bedingungsschlüssel für die AWS Support-App in Slack
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Support Plans
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS-Nachhaltigkeit
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Systems Manager
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Systems Manager für SAP
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Systems Manager GUI Connect
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Systems Manager Incident Manager
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Systems Manager Incident Manager Contacts
- Aktionen, Ressourcen und Bedingungsschlüssel für Tag-Editor
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Tax Settings
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Telco Network Builder
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Textract
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Timestream
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Timestream InfluxDB
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Tiros
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Transcribe
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Transfer Family
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Translate
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Trusted Advisor
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS User Notifications
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS User Notifications Contacts
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Verified Access
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Verified Permissions
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon VPC Lattice

- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon VPC Lattice Services
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS WAF
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS WAF Regional
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS WAF V2
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Well-Architected Tool
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Wickr
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon WorkDocs
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon WorkLink
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon WorkMail
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon WorkMail Message Flow
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon WorkSpaces
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon WorkSpaces Application Manager
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon WorkSpaces Thin Client
- Aktionen, Ressourcen und Bedingungsschlüssel für Amazon WorkSpaces Web
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS X-Ray

Aktionen, Ressourcen und Bedingungsschlüssel für AWS-Kontenverwaltung

AWS-Kontenverwaltung (Servicepräfix: `account`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS-Kontenverwaltung definierte Aktionen
- Von AWS-Kontenverwaltung definierte Ressourcentypen

- Bedingungsschlüssel für AWS-Kontenverwaltung

Von AWS-Kontenverwaltung definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CloseAccount [nur Berechtigung]	Gewährt die Berechtigung zum Schließen eines Kontos	Schreiben	account		
DeleteAlternateContact	Gewährt die Berechtigung zum Löschen der alternativen Kontakte für ein Konto	Schreiben	account		
			accountInOrganization		
				account:AlternateContactTypes	
DisableRegion	Gewährt die Berechtigung zum Deaktivieren der Verwendung einer Region	Schreiben	account		
			accountInOrganization		
				account:TargetRegion	
EnableRegion	Gewährt die Berechtigung der Verwendung zum Aktivieren einer Region	Schreiben	account		
			accountInOrganization		
				account:TargetRegion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAccountInformation [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen der Kontoinformationen für ein Konto	Lesen	account		
GetAlternateContact	Gewährt die Berechtigung zum Abrufen der alternativen Kontakte für ein Konto	Lesen	account		
			accountInOrganization		
				account:AlternateContactTypes	
GetChallengeQuestions [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen der Sicherheitsabfragen für ein Konto	Lesen	account		
GetContactInformation	Erteilung der Berechtigung zum Abrufen der Hauptkontaktinformationen für ein Konto	Lesen	account		
			accountInOrganization		
GetRegionOptStatus	Gewährt die Berechtigung zum Abrufen des Opt-in-Status einer Region	Lesen	account		
			accountInOrganization		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				account:TargetRegion	
ListRegions	Gewährt die Berechtigung zum Auflisten der verfügbaren Regionen	Auflisten	account		
			accountInOrganization		
PutAlternateContact	Gewährt die Berechtigung zum Ändern der alternativen Kontakte für ein Konto	Schreiben	account		
			accountInOrganization		
				account:AlternateContactTypes	
PutChallengeQuestions [nur Berechtigung]	Gewährt die Berechtigung zum Ändern der Sicherheitsabfragen für ein Konto	Schreiben	account		
PutContactInformation	Erteilung der Berechtigung zur Aktualisierung der primären Kontaktinformationen für ein Konto	Schreiben	account		
			accountInOrganization		

Von AWS-Kontenverwaltung definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
account	`arn:${Partition}:account::${Account}:account`	
accountInOrganization	`arn:${Partition}:account::${ManagementAccountId}:account/o-${OrganizationId}/${MemberAccountId}`	

Bedingungsschlüssel für AWS-Kontenverwaltung

AWS-Kontenverwaltung definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
account:AccountResourceOrgPaths	Filtert den Zugriff nach dem Ressourcenpfad für ein Konto in einer Organisation	ArrayOfString
account:AccountRes	Filtert den Zugriff nach Ressourcen-Tags für ein Konto in einer Organisation	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
ourceOrgTags/${TagKey}		
account:AlternateContactTypes	Filtert den Zugriff nach alternativen Kontakttypen	ArrayOfString
account:TargetRegion	Filtert den Zugriff nach einer Liste von Regionen. Aktiviert oder deaktiviert alle hier angegebenen Regionen	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Activate

AWS Activate (Servicepräfix: `activate`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Activate definierte Aktionen
- Von AWS Activate definierte Ressourcentypen
- Bedingungsschlüssel für AWS Activate

Von AWS Activate definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateForm	Gewährt die Berechtigung zum Übermitteln eines Activate-Antragsformulars	Write			
GetAccountContact	Gewährt die Berechtigung zum Abrufen der Kontaktinformationen für AWS-Konto	Read			
GetContentInfo	Gewährt die Berechtigung, technische Posts für Activate zu erhalten und Informationen bereitzustellen	Read			
GetCosts	Gewährt die Berechtigung zum Abrufen der AWS-Kosteninformationen	Read			
GetCredits	Gewährt die Berechtigung zum Abrufen der AWS-Guthabeninformationen	Read			
GetMemberInfo	Gewährt die Berechtigung zum Abrufen der Activate-Mitgliedsinformationen	Read			
GetProgram	Gewährt die Berechtigung zum Abrufen eines Activate-Programms	Read			
PutMemberInfo	Gewährt die Berechtigung zum Erstellen oder Aktualisieren der Activate-Mitgliedsinformationen	Write			

Von AWS Activate definierte Ressourcentypen

AWS Activate unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf AWS Activate zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Activate

Activate besitzt keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Alexa for Business

Alexa for Business (Servicepräfix: `a4b`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Alexa for Business definierte Aktionen
- Von Alexa for Business definierte Ressourcentypen
- Bedingungsschlüssel für Alexa for Business

Von Alexa for Business definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ApproveSkill	Gewährt die Erlaubnis, einen Skill der Organisation unter dem AWS-Konto des Kunden zuzuordnen	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateContactWithAddressBook	Gewährt die Erlaubnis, einen Kontakt mit einem bestimmten Adressbuch zu verknüpfen	Write	addressbook*		
			contact*		
AssociateDeviceWithNetworkProfile	Gewährt die Berechtigung, ein Gerät mit dem angegebenen Netzwerkprofil zu verknüpfen	Write	device*		
			networkprofile*		
AssociateDeviceWithRoom	Gewährt die Erlaubnis, ein Gerät mit einem bestimmten Raum zu verknüpfen	Write	device*		
			room*		
AssociateSkillGroupWithRoom	Gewährt die Erlaubnis, die Qualifikationsgruppe mit einem bestimmten Raum zu verknüpfen	Write	room*		
			skillgroup*		
AssociateSkillWithSkillGroup	Gewährt die Erlaubnis, einen Skill mit einer Qualifikationsgruppe zu verknüpfen	Write	skillgroup*		
AssociateSkillWithUsers	Gewährt die Erlaubnis einen privaten Skill für registrierte Benutzer bereitzustellen, damit diese ihn auf ihren Geräten aktivieren können	Write			
CompleteRegistration [nur Berechtigung]	Gewährt die Erlaubnis, den Vorgang der Registrierung eines Alexa-Geräts abzuschließen	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAddressBook	Gewährt die Berechtigung zum Erstellen eines Adressbuchs mit den angegebenen Details	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateBusinessReportSchedule	Gewährt die Erlaubnis, einen sich wiederholenden Zeitplan für Nutzungsberichte zu erstellen, die im täglichen oder wöchentlichen Intervall an den angegebenen S3-Speicherort bereitgestellt werden.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConferenceProvider	Gewährt die Berechtigung zum Hinzufügen eines neuen Konferenzanbieters unter dem AWS-Konto des Benutzers	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateContact	Gewährt die Berechtigung zum Erstellen eines Kontakts mit den angegebenen Details	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateGatewayGroup	Gewährt die Berechtigung zum Erstellen einer Gateway-Gruppe mit den angegebenen Details	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateNetworkProfile	Gewährt die Berechtigung zum Erstellen eines Netzwerkprofils mit den angegebenen Details	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfile	Gewährt die Berechtigung zum Erstellen eines neuen Profils	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRoom	Gewährt die Berechtigung zum Erstellen eines Raums mit den angegebenen Details	Write	profile*	aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSkillGroup	Gewährt die Berechtigung zum Erstellen einer Qualifikationsgruppe mit dem gegebenen Vornamen und der gegebenen Beschreibung	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateUser	Gewährt die Berechtigung zum Erstellen eines Benutzers	Write	user*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAddressBook	Gewährt die Berechtigung zum Löschen eines Adressbuchs anhand des Adressbuch-ARN	Write	addressbook*		
DeleteBusinessReportSchedule	Gewährt die Berechtigung zum Löschen des wiederkehrenden Zeitplans für die Bereitstellung des Berichts anhand des angegebenen Zeitplan-ARN	Write	schedule*		
DeleteConferenceProvider	Gewährt die Berechtigung zum Löschen eines Konferenzanbieters	Write	conferenceprovider*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteContact	Gewährt die Berechtigung, einen Kontakt durch den Kontak-ARN zu löschen	Write	contact*		
DeleteDevice	Gewährt die Erlaubnis, ein Gerät von Alexa For Business zu entfernen	Write	device*		
DeleteDeviceUsageData	Gewährt die Erlaubnis, den gesamten vorherigen Verlauf der Spracheingabedaten und der zugehörigen Antwortdaten des Geräts zu löschen	Write	device*		
DeleteGatewayGroup	Gewährt die Berechtigung zum Löschen einer Gateway-Gruppe	Write	gatewaygroup*		
DeleteNetworkProfile	Gewährt die Berechtigung zum Löschen eines Netzwerkprofils durch das Netzwerkprofil-ARN	Write	networkprofile*		
DeleteProfile	Gewährt die Berechtigung zum Löschen von Profilen nach Profil-ARN	Write	profile*		
DeleteRoom	Gewährt die Berechtigung zum Löschen von Räumen	Write	room*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteRoomSkillParameter	Gewährt die Berechtigung zum Löschen eines Parameters aus einer Qualifikation und einem Raum	Write	room*		
DeleteSkillAuthorization	Gewährt die Erlaubnis, ein Konto eines Drittanbieters von einem Skill aufzuheben	Write	room*		
DeleteSkillGroup	Gewährt die Berechtigung zum Löschen von Qualifikationsgruppen mit dem ARN der Qualifikationsgruppe	Write	skillgroup*		
DeleteUser	Gewährt die Berechtigung zum Löschen eines Benutzers	Write	user*		
DisassociateContactFromAddressBook	Gewährt die Erlaubnis, einen Kontakt von einem bestimmten Adressbuch zu trennen	Write	addressbook*		
			contact*		
DisassociateDeviceFromRoom	Gewährt die Erlaubnis, das Gerät von seinem aktuellen Raum zu trennen	Write	device*		
DisassociateSkillFromSkillGroup	Gewährt die Erlaubnis, einen Skill von einer Qualifikationsgruppe zu trennen	Write	skillgroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateSkillFromUsers	Gewährt die Berechtigung, eindn privaten Skill für registrierte Benutzer nicht mehr verfügbar zu machen und sie dann daran zu hindern, ihn auf ihren Geräten zu aktivieren	Write	user*		
DisassociateSkillGroupFromRoom	Gewährt die Erlaubnis, die Qualifikationsgruppe von einem bestimmten Raum zu trennen	Write	room* skillgroup*		
ForgetSmartHomeAppliances	Gewährt die Erlaubnis, Smart-Home-Geräte zu vergessen, die einem Raum zugeordnet sind	Write	room*		
GetAddressBook	Gewährt die Erlaubnis, die Adressbuchdetails anhand des Adressbuch-ARN zu erhalten	Read	addressbook*		
GetConferencePreference	Gewährt die Erlaubnis, die bestehenden Konferenz präferenzen abzurufen	Read			
GetConferenceProvider	Gewährt die Erlaubnis, Details zu einem bestimmten Konferenzanbieter zu erhalten	Read	conferenceprovider*		
GetContact	Gewährt die Erlaubnis, die Kontaktdetails durch den Kontakt-ARN zu erhalten	Read	contact*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDevice	Gewährt die Berechtigung zum Abrufen der Gerätedetails	Read	device*		
GetGateway	Gewährt die Berechtigung zum Abrufen der Details eines Gateways	Read	gateway*		
GetGatewayGroup	Gewährt die Berechtigung zum Abrufen der Details einer Gateway-Gruppe	Read	gatewaygroup*		
GetInvitationConfiguration	Gewährt die Berechtigung zum Abrufen der konfigurierten Werte für die E-Mail-Vorlage für die Einladung zur Benutzerregistrierung	Read			
GetNetworkProfile	Gewährt die Berechtigung zum Abrufen der Netzwerkprofildetails durch das Netzwerkprofil-ARN	Read	networkprofile*		
GetProfile	Gewährt die Berechtigung zum Abrufen von Profilen, wenn Profil-ARN bereitgestellt wird	Read	profile*		
GetRoom	Gewährt die Berechtigung zum Abrufen von Raumdetails	Read	room*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetRoomSkillParameter	Gewährt die Berechtigung zum Abrufen eines vorhandenen Parameters, der für eine Qualifikation und einen Raum eingestellt wurde	Read	room*		
GetSkillGroup	Gewährt die Berechtigung, mit dem ARN der Qualifikationsgruppe Details zu Qualifikationsgruppen zu erhalten	Read	skillgroup*		
ListBusinessReportSchedules	Gewährt die Berechtigung zum Auflisten der Details der Zeitpläne, die ein Benutzer konfiguriert hat	List			
ListConferenceProviders	Gewährt die Erlaubnis, Konferenzanbieter unter einem bestimmten AWS-Konto aufzulisten	List			
ListDeviceEvents	Gewährt die Berechtigung zum Auflisten des Geräteereignisverlaufs, einschließlich des Verbindungsstatus des Geräts, für bis zu 30 Tage	List	device*		
ListGatewayGroups	Gewährt die Berechtigung zum Auflisten von Gateway-Gruppen-Zusammenfassungen	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListGateways	Gewährt die Berechtigung zum Auflisten von Gateway-Zusammenfassungen	List	gatewaygroup*		
ListSkills	Gewährt die Berechtigung zum Auflisten von Skills	List			
ListSkillsStoreCategories	Gewährt die Berechtigung, alle Kategorien im Alexa Skill Store aufzulisten	List			
ListSkillsStoreSkillsByCategory	Gewährt die Erlaubnis, alle Skills im Alexa Skill Store nach Kategorie aufzulisten	List			
ListSmartHomeAppliances	Gewährt die Erlaubnis, alle mit einem Raum verbundenen Smart-Home-Geräte aufzulisten	List	room*		
ListTags	Gewährt die Berechtigung zum Auflisten aller Tags auf einer Ressource	Read	device		
			room		
			user		
PutConferencePreference	Gewährt die Berechtigung, die Konferenzeinstellungen eines bestimmten Konferenzanbieters auf der Kontoebene festzulegen	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutDeviceSetupEvents [nur Berechtigung]	Gewährt die Berechtigung zum Veröffentlichen von Alexa-Geräte-Setup-Ereignissen	Write			
PutInvitationConfiguration	Gewährt die Berechtigung zum Konfigurieren der E-Mail-Vorlage für die Benutzerregistrierungseinladung mit den angegebenen Attributen	Write			
PutRoomSkillParameter	Gewährt die Berechtigung zum Einstellen eines raumspezifischen Parameters für einen Skill	Write	room*		
PutSkillAuthorization	Gewährt die Berechtigung, das Benutzerkonto mit einem Skill-Drittanbieter zu verknüpfen	Write	room*		
RegisterAVSDevice	Gewährt die Berechtigung, ein Alexa-fähiges Gerät zu registrieren, das durch einen Originalgerätehersteller mithilfe von Alexa Voice Service (AVS) erstellt wurde.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
RegisterDevice [nur Berechtigung]	Gewährt die Erlaubnis, ein Alexa-Gerät zu registrieren	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RejectSkill	Gewährt die Berechtigung, einen Skill von der Organisation unter dem AWS-Konto eines Benutzers zu trennen	Write			
ResolveRoom	Gewährt die Erlaubnis, Rauminformationen zu lösen	Read			
RevokeInvitation	Gewährt die Berechtigung, eine Einladung zu widerrufen	Write	user*		
SearchAddressBooks	Gewährt die Berechtigung, Adressbücher zu durchsuchen und diejenigen aufzulisten, die eine Reihe von Filter- und Sortierkriterien erfüllen	List			
SearchContacts	Gewährt die Berechtigung, nach Kontakten zu suchen und diejenigen aufzulisten, die eine Reihe von Filter- und Sortierkriterien erfüllen	List			
SearchDevices	Gewährt die Berechtigung zum Suchen nach Geräten	List			
SearchNetworkProfiles	Gewährt die Berechtigung zum Suchen von Netzwerkprofilen und zum Auflisten derjenigen, die eine Reihe von Filter- und Sortierkriterien erfüllen	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SearchProfiles	Gewährt die Berechtigung zum Suchen nach Profilen	List			
SearchRooms	Gewährt die Berechtigung zum Suchen nach Räumen	List			
SearchSkillGroups	Gewährt die Berechtigung zum Suchen nach Qualifikationsgruppen	List			
SearchUsers	Gewährt die Berechtigung zum Suchen nach Benutzern	List			
SendAnnouncement	Gewährt die Berechtigung, einen asynchronen Ablauf auszulösen, um Text, SSML oder Audioankündigungen an Räume zu senden, die durch eine Suche oder einen Filter identifiziert werden	Write			
SendInvitation	Gewährt die Berechtigung, eine Einladung an einen Benutzer zu senden	Write	user*		
StartDeviceSync	Gewährt die Berechtigung, das Gerät und dessen Konto auf die bekannten Standardeinstellungen zurückzusetzen, indem alle Informationen und Einstellungen früherer Benutzer gelöscht werden	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartSmartHomeApplianceDiscovery	Gewährt die Berechtigung, die Erkennung aller Smart-Haushaltsgeräte zu starten, die mit dem Raum verknüpft sind	Read	room*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Metadaten-Tags zu einer Ressource	Markieren	device		
			room		
			user		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Metadaten-Tags aus einer Ressource	Markieren	device		
			room		
			user		
UpdateAddressBook	Gewährt die Berechtigung zum Aktualisieren der Adressbuchdetails durch den Adressbuch-ARN	Write	addressbook*		
UpdateBusinessReportSchedule	Gewährt die Berechtigung, die Konfiguration für die Bereitstellung des Berichts mit dem angegebenen Zeitplan-ARN zu aktualisieren	Write	schedule*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateConferenceProvider	Gewährt die Berechtigung, die Einstellungen eines bestehenden Konferenzanbieters zu aktualisieren	Write	conferenceprovider*		
UpdateContact	Gewährt die Berechtigung, die Kontaktdetails durch den Kontakt-ARN zu aktualisieren	Write	contact*		
UpdateDevice	Gewährt die Berechtigung zum Aktualisieren des Gerätenamens	Write	device*		
UpdateGateway	Gewährt die Berechtigung zum Aktualisieren der Details eines Gateways	Write	gateway*		
UpdateGatewayGroup	Gewährt die Berechtigung zum Aktualisieren der Details einer Gateway-Gruppe	Write	gatewaygroup*		
UpdateNetworkProfile	Gewährt die Berechtigung zum Aktualisieren eines Netzwerkprofils durch das Netzwerkprofil-ARN	Write	networkprofile*		
UpdateProfile	Gewährt die Berechtigung zum Aktualisieren eines vorhandenen Profils	Write	profile*		
UpdateRoom	Gewährt die Berechtigung zum Aktualisieren von Raumdetails	Write	room*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateSkillGroup	Gewährt die Berechtigung zum Aktualisieren von Qualifikationsgruppendetails mit dem ARN der Qualifikationsgruppe	Write	skillgroup*		

Von Alexa for Business definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
profile	`arn:${Partition}:a4b:${Region}:${Account}:profile/${ResourceId}`	
room	`arn:${Partition}:a4b:${Region}:${Account}:room/${ResourceId}`	aws:ResourceTag/${TagKey}
device	`arn:${Partition}:a4b:${Region}:${Account}:device/${ResourceId}`	aws:ResourceTag/${TagKey}
skillgroup	`arn:${Partition}:a4b:${Region}:${Account}:skill-group/${ResourceId}`	
user	`arn:${Partition}:a4b:${Region}:${Account}:user/${ResourceId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
addressbook	`arn:${Partition}:a4b:${Region}:${Account}:address-book/${ResourceId}`	
conferenceprovider	`arn:${Partition}:a4b:${Region}:${Account}:conference-provider/${ResourceId}`	
contact	`arn:${Partition}:a4b:${Region}:${Account}:contact/${ResourceId}`	
schedule	`arn:${Partition}:a4b:${Region}:${Account}:schedule/${ResourceId}`	
networkprofile	`arn:${Partition}:a4b:${Region}:${Account}:network-profile/${ResourceId}`	
gateway	`arn:${Partition}:a4b:${Region}:${Account}:gateway/${ResourceId}`	
gatewaygroup	`arn:${Partition}:a4b:${Region}:${Account}:gateway-group/${ResourceId}`	

Bedingungsschlüssel für Alexa for Business

Alexa for Business definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
a4b:amazonId	Filtert Aktionen basierend auf der Amazon-ID in der Anforderung	Zeichenfolge
a4b:filters_deviceType	Filtert Aktionen auf Grundlage des Gerätetyps in der Anforderung	ArrayOfString
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf den zulässigen Werten für die einzelnen Tags	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf dem Tag-Wert, der der Ressource zugeordnet ist	Zeichenfolge
aws:TagKeys	Filtert Aktionen basierend auf den obligatorischen Tags in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AmazonMediaImport

AmazonMediaImport (Service-Präfix: `mediaimport`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AmazonMediaImport definierte Aktionen
- Von AmazonMediaImport definierte Ressourcentypen
- Bedingungsschlüssel für AmazonMediaImport

Von AmazonMediaImport definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDatabaseBinarySnapshot [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines binären Snapshots der Datenbank für das AWS-Konto des Kunden	Schreiben			

Von AmazonMediaImport definierte Ressourcentypen

AmazonMediaImport unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf AmazonMediaImport zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AmazonMediaImport

mediaimport besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Amplify

AWS Amplify (Servicepräfix: `amplify`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Amplify definierte Aktionen

- Von AWS Amplify definierte Ressourcentypen
- Bedingungsschlüssel für AWS Amplify

Von AWS Amplify definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateApp	Gewährt die Berechtigung zum Erstellen einer neuen Amplify App	Schreiben	apps*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBackendEnvironment	Gewährt die Berechtigung zum Erstellen einer neuen Backend-Umgebung für ein Amplify App	Schreiben	apps*		
CreateBranch	Gewährt die Berechtigung zum Erstellen eines neuen Branch für ein Amplify App	Schreiben	apps*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeployment	Gewährt die Berechtigung zum Erstellen einer Bereitstellung für Anwendungen zur manuellen Bereitstellung. (Apps sind nicht mit dem Repository verbunden.)	Schreiben	branches*		
	Gewährt die Berechtigung zum Erstellen einer neuen	Schreiben	apps*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDomainAssociation	DomainAssociation in einer App			aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebHook	Gewährt die Berechtigung zum Erstellen eines neuen Webhook in einer App	Schreiben	branches*		
DeleteApp	Gewährt die Berechtigung zum Löschen einer vorhandenen Amplify App nach appId	Schreiben	apps*		
DeleteBackendEnvironment	Gewährt die Berechtigung zum Löschen eines neuen Branch für ein Amplify App	Schreiben	apps*		
DeleteBranch	Gewährt die Berechtigung zum Löschen eines neuen Branch für ein Amplify App	Schreiben	branches*		
DeleteDomainAssociation	Gewährt die Berechtigung zum Löschen einer DomainAssociation	Schreiben	domains*		
DeleteJob	Gewährt die Berechtigung zum Löschen eines Auftrags für einen Amplify-Branch, Teil der Amplify App	Schreiben	jobs*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteWebHook	Gewährt die Berechtigung zum Löschen eines Webhook nach ID	Schreiben	webhooks*		
GenerateAccessLogs	Gewährt die Berechtigung zum Generieren von Website-Zugriffsprotokollen für einen bestimmten Zeitraum über eine vorsignierte URL	Schreiben	apps*		
GetApp	Gewährt die Berechtigung zum Abrrufen einer vorhanden en Amplify App nach appId	Lesen	apps*		
GetArtifactUrl	Gewährt die Berechtigung zum Abrufen von Artefakt-Informationen, die einer ArtifactId entsprechen	Lesen	apps*		
GetBackendEnvironment	Gewährt die Berechtigung zum Abrufen einer Backend-Umgebung für ein Amplify App	Lesen	apps*		
GetBranch	Gewährt die Berechtigung zum Abrufen eines neuen Branch für ein Amplify App	Lesen	branches*		
GetDomainAssociation	Gewährt die Berechtigung zum Abrufen von Domain-Informationen, die einer App-ID und einem Domain-Namen entsprechen	Lesen	domains*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetJob	Gewährt die Berechtigung zum Erhalten eines Auftrags für einen Branch, Teil einer Amplify App	Lesen	jobs*		
GetWebHook	Gewährt die Berechtigung zum Abrufen von Webhook-Informationen, die einer Webhook-ID entsprechen	Lesen	webhooks*		
ListApps	Gewährt die Berechtigung zum Auflisten vorhandener Amplify Apps	Auflisten			
ListArtifacts	Gewährt die Berechtigung zum Auflisten von Artefakten mit einer App, einem Branch, einem Auftrag und einem Artefakttyp	Auflisten	apps*		
ListBackendEnvironments	Gewährt die Berechtigung zum Auflisten der Backend-Umgebungen für eine Amplify app	Auflisten	apps*		
ListBranches	Gewährt die Berechtigung zum Auflisten von Branches für eine Amplify App	Auflisten	apps*		
ListDomainAssociations	Gewährt die Berechtigung zum Auflisten von Domains mit einer App	Auflisten	apps*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListJobs	Gewährt die Berechtigung zum Erhalten von Aufträgen für einen Branch, Teil einer Amplify App	Auflisten	branches*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine AWS-Amplify-Console-Ressource	Lesen	apps		
			branches		
			domains		
			webhooks		
ListWebHooks	Gewährt die Berechtigung zum Auflisten von Webhooks in einer App	Auflisten	apps*		
StartDeployment	Gewährt die Berechtigung zum Starten einer Bereitstellung für Anwendungen zur manuellen Bereitstellung. (Apps sind nicht mit dem Repository verbunden.)	Schreiben	branches*		
StartJob	Gewährt die Berechtigung zum Starten eines neuen Auftrags für einen Branch, Teil einer Amplify App	Schreiben	jobs*		
StopJob	Gewährt die Berechtigung zum Beenden eines Auftrags, der gerade ausgeführt wird, für einen Amplify-Branch, Teil der Amplify App	Schreiben	jobs*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Markieren einer AWS-Amplify-Console-Ressource	Markierung	apps		
			branches		
			domains		
			webhooks		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen eines Tags aus einer AWS-Amplify-Console-Ressource	Markierung	apps		
			branches		
			domains		
			webhooks		
				aws:TagKeys	
UpdateApp	Gewährt die Berechtigung zum Aktualisieren einer vorhanden Amplify-App	Schreiben	apps*		
UpdateBranch	Gewährt die Berechtigung zum Aktualisieren eines neuen Branch für eine Amplify-App	Schreiben	branches*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateDomainAssociation	Gewährt die Berechtigung zum Aktualisieren einer DomainAssociation in einer App	Schreiben	domains*		
UpdateWebHook	Gewährt die Berechtigung zum Aktualisieren eines Webhook	Schreiben	webhooks*		

Von AWS Amplify definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
apps	`arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}`	aws:ResourceTag/${TagKey}
branches	`arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}/branches/${BranchName}`	aws:ResourceTag/${TagKey}
jobs	`arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}/branches/${BranchName}/jobs/${JobId}`	

Ressourcentypen	ARN	Bedingungsschlüssel
domains	`arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}/domains/${DomainName}`	aws:ResourceTag/${TagKey}
webhooks	`arn:${Partition}:amplify:${Region}:${Account}:webhooks/${WebhookId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Amplify

AWS Amplify definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Schlüssel eines Tags und den Wert einer Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Tag-Schlüssel, der der Ressource zugeordnet ist	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach den Tag-Schlüsseln in einer Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Amplify Admin

AWS Amplify Admin (Servicepräfix: `amplifybackend`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Amplify Admin definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CloneBackend	Gewährt die Berechtigung zum Klonen einer vorhandenen Amplify Admin-Backend-Umgebung in eine neue Amplify Admin-Backend-Umgebung	Write	backend*		
CreateBackend	Gewährt die Berechtigung zum Erstellen einer neuen Amplify Admin-Backend-Umgebung nach Amplify-appId	Schreiben	created-backend*		
CreateBackendAPI	Gewährt die Berechtigung zum Erstellen einer API für	Schreiben	api*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	eine vorhandene Amplify Admin-Backend-Umgebung nach appId und backendEnvironmentName		backend*		
			environment*		
CreateBackendAuth	Gewährt die Berechtigung zum Erstellen einer Authentifizierungsressource für eine vorhandene Amplify Admin-Backend-Umgebung nach appId und backendEnvironmentName	Schreiben	auth*		
			backend*		
			environment*		
CreateBackendConfig	Gewährt die Berechtigung zum Erstellen einer neuen Amplify Admin-Backend-Konfiguration nach Amplify-appId	Schreiben	config*		
CreateBackendStorage	Gewährt die Berechtigung zum Erstellen einer Backend-Speicherressource	Schreiben	backend*		
			environment*		
			storage*		
CreateToken	Gewährt die Berechtigung zum Erstellen eines Amplify Admin-Abfrage-Tokens nach appId	Schreiben	backend*		
			token*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteBackend	Gewährt die Berechtigung zum Löschen einer vorhandenen Amplify Admin-Backend-Umgebung nach appId und backendEnvironmentName	Schreiben	backend*		
			environment*		
DeleteBackendAPI	Gewährt die Berechtigung zum Löschen einer API einer vorhandenen Amplify Admin-Backend-Umgebung nach appId und backendEnvironmentName	Schreiben	api*		
			backend*		
			environment*		
DeleteBackendAuth	Gewährt die Berechtigung zum Löschen einer Authentifizierungsressource einer vorhandenen Amplify Admin-Backend-Umgebung nach appId und backendEnvironmentName	Schreiben	auth*		
			backend*		
			environment*		
DeleteBackendStorage	Gewährt die Berechtigung zum Löschen einer Backend-Speicherressource	Schreiben	backend*		
			environment*		
			storage*		
DeleteToken	Gewährt die Berechtigung zum Löschen eines Amplify Admin-Abfrage-Tokens nach appId	Schreiben	backend*		
			token*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GenerateBackendAPIModels	Gewährt die Berechtigung zum Generieren von Modellen für eine API einer vorhandenen Amplify Admin-Backend-Umgebung nach appId und backendEnvironmentName	Schreiben	api*		
			backend*		
			environment*		
GetBackend	Gewährt die Berechtigung zum Abrufen einer vorhandenen Amplify Admin-Backend-Umgebung nach appId und backendEnvironmentName	Lesen	backend*		
			environment*		
GetBackendAPI	Gewährt die Berechtigung zum Abrufen einer API einer vorhandenen Amplify Admin-Backend-Umgebung nach appId und backendEnvironmentName	Lesen	api*		
			backend*		
			environment*		
GetBackendAPIModels	Gewährt die Berechtigung zum Abrufen von Modellen für eine API einer vorhandenen Amplify Admin-Backend-Umgebung nach appId und backendEnvironmentName	Lesen	api*		
			backend*		
			environment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBackendAuth	Gewährt die Berechtigung zum Abrufen einer Authentifizierungsressource einer vorhandenen Amplify Admin-Backend-Umgebung nach appId und backendEnvironmentName	Lesen	auth*		
			backend*		
			environment*		
GetBackendJob	Gewährt die Berechtigung zum Abrufen eines Auftrags einer vorhandenen Amplify Admin-Backend-Umgebung nach appId und backendEnvironmentName	Lesen	backend*		
			job*		
GetBackendStorage	Gewährt die Berechtigung zum Abrufen einer vorhandenen Backend-Speicherressource	Lesen	backend*		
			environment*		
GetToken	Gewährt die Berechtigung zum Abrufen eines Amplify Admin-Abfrage-Tokens nach appId	Lesen	backend*		
			token*		
ImportBackendAuth	Gewährt die Berechtigung zum Importieren einer vorhandenen Authentifizierungsressource einer Amplify Admin-Backend-Umgebung nach appId und backendEnvironmentName	Schreiben	auth*		
			backend*		
			environment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ImportBackendStorage	Gewährt die Berechtigung zum Importieren einer vorhandenen Backend-Speicherressource	Schreiben	backend*		
			environment*		
			storage*		
ListBackendJobs	Gewährt die Berechtigung zum Abrufen der Aufträge einer vorhandenen Amplify Admin-Backend-Umgebung nach appId und backendEnvironmentName	Auflisten	backend*		
			job*		
ListS3Buckets	Gewährt die Berechtigung zum Abrufen von S3-Buckets	Auflisten			
RemoveAllBackends	Gewährt die Berechtigung zum Löschen aller vorhandenen Amplify Admin-Backend-Umgebungen nach appId	Write	backend*		
			environment*		
RemoveBackendConfig	Gewährt die Berechtigung zum Löschen einer Amplify Admin-Backend-Konfiguration nach Amplify-appId	Schreiben	config*		
UpdateBackendAPI	Gewährt die Berechtigung zum Aktualisieren einer API einer vorhandenen Amplify Admin-Backend-Umgebung nach appId und backendEnvironmentName	Schreiben	api*		
			backend*		
			environment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateBackendAuth	Gewährt die Berechtigung zum Aktualisieren einer Authentifizierungsressource einer vorhandenen Amplify Admin-Backend-Umgebung nach appId und backendEnvironmentName	Schreiben	auth*		
			backend*		
			environment*		
UpdateBackendConfig	Gewährt die Berechtigung zum Aktualisieren einer Amplify Admin-Backend-Konfiguration nach Amplify-appId	Schreiben	config*		
UpdateBackendJob	Gewährt die Berechtigung zum Aktualisieren eines Auftrags einer vorhandenen Amplify Admin-Backend-Umgebung nach appId und backendEnvironmentName	Schreiben	backend*		
			job*		
UpdateBackendStorage	Gewährt die Berechtigung zum Aktualisieren einer Backend-Speicherressource	Schreiben	backend*		
			environment*		
			storage*		

Von AWS Amplify Admin definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
created-backend	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/*`	
backend	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/*`	
environment	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/environments/*`	
api	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/api/*`	
auth	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/auth/*`	
job	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/job/*`	
config	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/config/*`	
token	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/challenge/*`	
storage	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/storage/*`	

Bedingungsschlüssel für AWS Amplify Admin

Amplify Admin umfasst keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Amplify UI Builder

AWS Amplify UI Builder (Servicepräfix: `amplifyuibuilder`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Amplify UI Builder definierte Aktionen
- Von AWS Amplify UI Builder definierte Ressourcentypen
- Bedingungsschlüssel für AWS Amplify UI Builder

Von AWS Amplify UI Builder definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWSzu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn

die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateComponent	Gewährt die Berechtigung zum Erstellen einer Komponente	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	amplify:GetApp amplifyuibuilder:GetComponent

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					amplifyuibuilder:TagResource
CreateForm	Gewährt die Berechtigung zum Erstellen eines Formulars	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	amplify:GetApp amplifyuibuilder:GetForm amplifyuibuilder:TagResource amplifyuibuilder:UntagResource
CreateTheme	Gewährt die Berechtigung zum Erstellen eines Designs	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	amplify:GetApp amplifyuibuilder:GetTheme amplifyuibuilder:TagResource

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteComponent	Gewährt die Berechtigung zum Löschen einer Komponente	Schreiben	ComponentResource*		amplify:GetApp amplifyuibuilder:UntagResource
DeleteForm	Gewährt die Berechtigung zum Löschen eines Formulars	Schreiben	FormResource*		amplify:GetApp amplifyuibuilder:TagResource amplifyuibuilder:UntagResource
DeleteTheme	Gewährt die Berechtigung zum Löschen eines Designs	Schreiben	ThemeResource*		amplify:GetApp amplifyuibuilder:UntagResource
ExchangeCodeForToken	Gewährt die Berechtigung zum Austauschen eines Codes gegen ein Token	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ExportComponents	Gewährt die Berechtigung zum Exportieren von Komponenten	Lesen			
ExportForms	Gewährt die Berechtigung zum Exportieren von Formularen	Lesen			
ExportThemes	Gewährt die Berechtigung zum Exportieren von Designs	Lesen			
GetCodegenJob	Gewährt die Berechtigung zum Abrufen eines vorhandenen Codegen-Auftrags	Lesen	CodegenJobResource*		amplify:GetApp
GetComponent	Gewährt die Berechtigung zum Abrufen einer bestehenden Komponente	Lesen	ComponentResource*		amplify:GetApp
GetForm	Gewährt die Berechtigung zum Abrufen eines bestehenden Formulars	Lesen	FormResource*		amplify:GetApp
GetMetadata	Gewährt die Berechtigung zum Abrufen vorhandener Metadaten	Lesen			
GetTheme	Gewährt die Berechtigung zum Abrufen eines bestehendes Designs	Lesen	ThemeResource*		amplify:GetApp
ListCodegenJobs	Gewährt die Berechtigung zum Auflisten eines vorhandenen Codegen-Auftrags	Auflisten			amplify:GetApp

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListComponents	Gewährt Berechtigung zum Auflisten von Testkomponenten	Auflisten			amplify:GetApp
ListForms	Gewährt die Berechtigung zum Auflisten von Formularen	Auflisten			amplify:GetApp
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für einen angegebenen Amazon-Ressourcennamen (ARN)	Auflisten	CodegenJobResource		
			ComponentResource		
			FormResource		
			ThemeResource		
ListThemes	Gewährt die Berechtigung zum Auflisten der Themen	Auflisten			amplify:GetApp
PutMetadataFlag	Gewährt die Berechtigung zum Platzieren von vorhandenen Metadaten	Schreiben			
RefreshToken	Gewährt die Berechtigung zum Aktualisieren eines Zugriffstokens	Schreiben			
ResetMetadataFlag	Gewährt die Berechtigung zum Zurücksetzen vorhandener Metadaten	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartCodegenJob	Gewährt die Berechtigung zum Starten eines vorhandenen Codegen-Auftrags	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	amplify:GetApp
TagResource	Gewährt die Berechtigung zum Markieren der Ressource mit einem Tag-Schlüssel und -Wert	Tagging	CodegenJobResource		
			ComponentResource		
			FormResource		
			ThemeResource		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource mit einem angegebenen Amazon-Ressourcennamen (ARN)	Tagging	CodegenJobResource		
			ComponentResource		
			FormResource		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			ThemeResource		
				aws:TagKeys	
UpdateComponent	Gewährt die Berechtigung zum Aktualisieren einer Komponente	Schreiben	ComponentResource*		amplify:GetApp amplifyuibuilder:TagResource amplifyuibuilder:UntagResource

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateForm	Gewährt die Berechtigung zum Aktualisieren eines Formulars	Schreiben	FormResource*		amplify:GetApp amplifyuibuilder:GetForm amplifyuibuilder:TagResource amplifyuibuilder:UntagResource
UpdateTheme	Gewährt die Berechtigung zum Aktualisieren eines Designs	Schreiben	ThemeResource*		amplify:GetApp amplifyuibuilder:GetTheme amplifyuibuilder:TagResource amplifyuibuilder:UntagResource

Von AWS Amplify UI Builder definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
CodegenJobResource	`arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/environment/${EnvironmentName}/codegen-jobs/${Id}`	amplifyuibuilder:CodegenJobResourceAppId amplifyuibuilder:CodegenJobResourceEnvironmentName amplifyuibuilder:CodegenJobResourceId aws:ResourceTag/${TagKey}
ComponentResource	`arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/environment/${EnvironmentName}/components/${Id}`	amplifyuibuilder:ComponentResourceAppId amplifyuibuilder:ComponentResourceEnvironmentName amplifyuibuilder:ComponentResourceId

Ressourcentypen	ARN	Bedingungsschlüssel
		aws:ResourceTag/${TagKey}
FormResource	arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/environment/${EnvironmentName}/forms/${Id}	amplifyuibuilder:FormResourceAppId amplifyuibuilder:FormResourceEnvironmentName amplifyuibuilder:FormResourceId aws:ResourceTag/${TagKey}
ThemeResource	arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/environment/${EnvironmentName}/themes/${Id}	amplifyuibuilder:ThemeResourceAppId amplifyuibuilder:ThemeResourceEnvironmentName amplifyuibuilder:ThemeResourceId aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Amplify UI Builder

AWS Amplify UI Builder definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
amplifyuibuilder:CodegenJobResourceAppId	Filtert den Zugriff anhand der App-ID	String
amplifyuibuilder:CodegenJobResourceEnvironmentName	Filtert den Zugriff nach dem Backend-Umgebungsnamen	String
amplifyuibuilder:CodegenJobResourceId	Filtert den Zugriff anhand der Codegen-Auftrags-ID	String
amplifyuibuilder:ComponentResourceAppId	Filtert den Zugriff anhand der App-ID	String
amplifyuibuilder:ComponentResourceEnvironmentName	Filtert den Zugriff nach dem Backend-Umgebungsnamen	String
amplifyuibuilder:ComponentResourceId	Filtert den Zugriff nach der Komponenten-ID	String

Bedingungsschlüssel	Beschreibung	Typ
amplifyuibuilder:FormResourceAppId	Filtert den Zugriff anhand der App-ID	String
amplifyuibuilder:FormResourceEnvironmentName	Filtert den Zugriff nach dem Backend-Umgebungsnamen	String
amplifyuibuilder:FormResourceId	Filtert den Zugriff anhand der Formular-ID	String
amplifyuibuilder:ThemeResourceAppId	Filtert den Zugriff anhand der App-ID	String
amplifyuibuilder:ThemeResourceEnvironmentName	Filtert den Zugriff nach dem Backend-Umgebungsnamen	String
amplifyuibuilder:ThemeResourceId	Filtert den Zugriff anhand der Design-ID	String
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Apache-Kafka-APIs für Amazon-MSK-Cluster

Apache-Kafka-APIs für Amazon-MSK-Cluster (Service-Prefix: `kafka-cluster`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Apache-Kafka-APIs für Amazon-MSK-Cluster definierte Aktionen
- Von Apache-Kafka-APIs für Amazon-MSK-Cluster definierte Ressourcentypen
- Bedingungsschlüssel für Apache-Kafka-APIs für Amazon-MSK-Cluster

Von Apache-Kafka-APIs für Amazon-MSK-Cluster definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AlterCluster	Gewährt die Berechtigung zum Ändern verschiedener Aspekte des Clusters, was der ALTER-CLUSTER-ACL von Apache Kafka entspricht	Write	cluster*		kafka-cluster:Connect kafka-cluster:DescribeCluster
AlterClusterDynamicConfiguration	Gewährt die Berechtigung zum Ändern der dynamischen Konfiguration eines Clusters, was der ALTER_CONFIGS-CLUSTER-ACL von Apache Kafka entspricht	Write	cluster*		kafka-cluster:Connect kafka-cluster:DescribeClusterDynamicConfiguration
AlterGroup	Gewährt die Erlaubnis, Gruppen in einem Cluster beizutreten, was der READ GROUP ACL von Apache Kafka entspricht	Write	group*		kafka-cluster:Connect kafka-cluster:DescribeGroup
AlterTopic	Gewährt die Berechtigung zum Ändern von Themen auf einem Cluster, was der ALTER-TOPIC-ACL von Apache Kafka entspricht	Write	topic*		kafka-cluster:Connect

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					kafka-cluster:DescribeTopic
AlterTopicDynamicConfiguration	Gewährt die Berechtigung zum Ändern der dynamischen Konfiguration von Themen auf einem Cluster, was der ALTER_CONFIGS-TOPICY-ACL von Apache Kafka entspricht	Write	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopicDynamicConfiguration
AlterTransactionalId	Gewährt die Berechtigung zum Ändern der Transaktions-IDs auf einem Cluster, was der WRITE-TRANSACTIONAL_ID-ACL von Apache Kafka entspricht	Write	transactional-id*		kafka-cluster:Connect kafka-cluster:DescribeTransactionalId kafka-cluster:WriteData
Connect	Gewährt die Berechtigung, sich mit dem Cluster zu verbinden und zu authentifizieren	Write	cluster*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTopic	Gewährt die Berechtigung zum Erstellen von Themen auf einem Cluster, was der CREATE-CLUSTER/TOPIC-ACL von Apache Kafka entspricht	Write	topic*		kafka-cluster:Connect
DeleteGroup	Gewährt die Berechtigung zum Löschen von Gruppen auf einem Cluster, was der DELETE-GROUP-ACL von Apache Kafka entspricht	Write	group*		kafka-cluster:Connect kafka-cluster:DescribeGroup
DeleteTopic	Gewährt die Berechtigung zum Löschen von Themen auf einem Cluster, was der DELETE TOPICL von Apache Kafka entspricht	Write	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopic
DescribeCluster	Gewährt die Berechtigung zum Beschreiben verschiedener Aspekte des Clusters, was der DESCRIBE-CLUSTER-ACL von Apache Kafka entspricht	List	cluster*		kafka-cluster:Connect

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeClusterDynamicConfiguration	Gewährt die Berechtigung zum Beschreiben der dynamischen Konfiguration eines Clusters, was der DESCRIBE_CONFIGS-CLUSTER-ACL von Apache Kafka entspricht	List	cluster*		kafka-cluster:Connect
DescribeGroup	Gewährt die Berechtigung zum Beschreiben von Gruppen auf einem Cluster, was der DESCRIBE-GROUP-ACL von Apache Kafka entspricht	List	group*		kafka-cluster:Connect
DescribeTopic	Gewährt die Berechtigung zum Beschreiben von Themen auf einem Cluster, was der CONSMISSION-TOPICLE-ACL von Apache Kafka entspricht	List	topic*		kafka-cluster:Connect
DescribeTopicDynamicConfiguration	Gewährt die Berechtigung zum Beschreiben der dynamischen Konfiguration von Themen auf einem Cluster, was der RECRIEBE_CONFIGS-TOPIC-ACL von Apache Kafka entspricht	List	topic*		kafka-cluster:Connect

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeTransactionalId	Gewährt die Berechtigung zum Beschreiben der Transaktions-IDs auf einem Cluster, was der DESCRIBE-TRANSACTIONAL_ID-ACL von Apache Kafka entspricht	List	transactional-id*		kafka-cluster:Connect
ReadData	Gewährt die Berechtigung zum Lesen von Daten aus Themen auf einem Cluster, was der READ-TOPIC-ACL von Apache Kafka entspricht	Read	topic*		kafka-cluster:AlterGroup kafka-cluster:Connect kafka-cluster:DescribeTopic
WriteData	Gewährt die Berechtigung zum Schreiben von Daten zu Themen auf einem Cluster, was der WRITE-TOPIC-ACL von Apache Kafka entspricht	Write	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopic

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
WriteDataIdempotently	Gewährt die Berechtigung zum idempotenten Schreiben von Daten auf einen Cluster, was der IDEMPOTENT_WRITE-CLUSTER-ACL von Apache Kafka entspricht	Write	cluster*		kafka-cluster:Connect kafka-cluster:WriteData

Von Apache-Kafka-APIs für Amazon-MSK-Cluster definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
cluster	`arn:${Partition}:kafka:${Region}:${Account}:cluster/${ClusterName}/${ClusterUuid}`	aws:ResourceTag/${TagKey}
topic	`arn:${Partition}:kafka:${Region}:${Account}:topic/${ClusterName}/${ClusterUuid}/${TopicName}`	
group	`arn:${Partition}:kafka:${Region}:${Account}:group/${ClusterName}/${ClusterUuid}/${GroupName}`	

Ressourcentypen	ARN	Bedingungsschlüssel
transactional-id	`arn:${Partition}:kafka:${Region}:${Account}:transactional-id/${ClusterName}/${ClusterUuid}/${TransactionalId}`	

Bedingungsschlüssel für Apache-Kafka-APIs für Amazon-MSK-Cluster

Apache-Kafka-APIs für Amazon-MSK-Cluster definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf den Tag-Schlüssel-Wert-Paaren, die der Ressource angefügt wurden. Der Kontextschlüssel des Ressourcen-Tag gilt nur für die Cluster-Ressource, nicht für Themen, Gruppen und Transaktions-IDs	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon API Gateway

Amazon API Gateway (Servicepräfix: `execute-api`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.

- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon API Gateway definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
InvalidateCache	Macht den API-Cache auf Client-Anforderung ungültig	Write	execute-api-general*		
Invoke	Ruft auf Client-Anforderung eine API auf	Write	execute-api-general*		
ManageConnections	ManageConnections steuert den Zugriff auf die @connections-API.	Write	execute-api-general*		

Von Amazon API Gateway definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
execute-api-general	`arn:${Partition}:execute-api:${Region}:${Account}:${ApiId}/${Stage}/${Method}/${ApiSpecificResourcePath}`	

Bedingungsschlüssel für Amazon API Gateway

ExecuteAPI besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon-API-Gateway-Management

Amazon-API-Gateway-Management (Servicepräfix: `apigateway`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon-API-Gateway-Management definierte Aktionen
- Von Amazon-API-Gateway-Management definierte Ressourcentypen
- Bedingungsschlüssel für Amazon-API-Gateway-Management

Von Amazon-API-Gateway-Management definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddCertificateToDomain	Gewährt die Berechtigung zum Hinzufügen von Zertifikaten für die gegenseitige TLS-Authentifizierung zu einem Domainnamen. Dies ist eine zusätzliche Autorisierungskontrolle für die Verwaltung der DomainName Ressource, da mTLs sensibel sind.	Berechtigungsverwaltung	DomainName		
			DomainNames		
DELETE	Gewährt die Berechtigung zum Löschen einer bestimmten Ressource	Write	ApiKey		
			Authorizer		
			BasePathMapping		
			ClientCertificate		
			Deployment		
			DocumentationPart		
			DocumentationVersion		
			DomainName		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			GatewayResponse		
			Integration		
			IntegrationResponse		
			Method		
			MethodResponse		
			Model		
			RequestValidator		
			Resource		
			RestApi		
			Stage		
			Tags		
			Template		
			UsagePlan		
			UsagePlanKey		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			VpcLink		
				aws:RequestTag/${TagKey} aws:TagKeys	
GET	Gewährt die Berechtigung zum Lesen einer bestimmten Ressource	Read	Account		
			ApiKey		
			ApiKeys		
			Authorizer		
			Authorizers		
			BasePathMapping		
			BasePathMappings		
			ClientCertificate		
			ClientCertificates		
			Deployment		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			Deployments		
			DocumentationPart		
			DocumentationParts		
			DocumentationVersion		
			DocumentationVersions		
			DomainName		
			DomainNames		
			GatewayResponse		
			GatewayResponses		
			Integration		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			IntegrationResponse		
			Method		
			MethodResponse		
			Model		
			Models		
			RequestValidator		
			RequestValidators		
			Resource		
			Resources		
			RestApi		
			RestApis		
			Sdk		
			Stage		
			Stages		
			Tags		
			UsagePlan		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			UsagePlanKey		
			UsagePlanKeys		
			UsagePlans		
			VpcLink		
			VpcLinks		
PATCH	Gewährt die Berechtigung zum Aktualisieren einer bestimmten Ressource	Write	Account		
			ApiKey		
			Authorizer		
			BasePathMapping		
			ClientCertificate		
			Deployment		
			DocumentationPart		
			DocumentationVersion		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			DomainName		
			GatewayResponse		
			Integration		
			IntegrationResponse		
			Method		
			MethodResponse		
			Model		
			RequestValidator		
			Resource		
			RestApi		
			Stage		
			Template		
			UsagePlan		
			UsagePlanKey		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			VpcLink		
				aws:RequestTag/${TagKey} aws:TagKeys	
POST	Gewährt die Berechtigung zum Erstellen einer bestimmten Ressource	Write	ApiKeys		
			Authorizers		
			BasePathMappings		
			ClientCertificates		
			Deployments		
			DocumentationParts		
			DocumentationVersions		
			DomainNames		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			GatewayResponses		
			IntegrationResponse		
			MethodResponse		
			Models		
			RequestValidators		
			Resources		
			RestApis		
			Stages		
			UsagePlanKeys		
			UsagePlans		
			VpcLinks		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PUT	Gewährt die Berechtigung zum Aktualisieren einer bestimmten Ressource	Write	DocumentationPart		
			GatewayResponse		
			IntegrationResponse		
			MethodResponse		
			RestApi		
			Tags		
				aws:RequestTag/${TagKey} aws:TagKeys	
RemoveCertificateFromDomain	Gewährt die Berechtigung zum Entfernen von Zertifikaten für die gegenseitige TLS-Authentifizierung von einem Domainnamen. Aufgrund der sensiblen Natur von mTLs handelt es sich um eine zusätzliche Autorisierungskontrolle für die Verwaltung der DomainName Ressource	Berechtigungsverwaltung	DomainName		
			DomainNames		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SetWebACL	Gewährt die Berechtigung, eine WAF-Zugriffssteuerungsliste (ACL) festzulegen. Dies ist eine zusätzliche Autorisierungskontrolle für die Verwaltung der Stage-Ressource, da es sich um sensible Daten handelt WebAcl	Berechtigungsverwaltung	Stage		
			Stages		
UpdateRestApiPolicy	Gewährt die Berechtigung zum Verwalten der IAM-Ressourcenrichtlinie für eine API. Dies ist eine zusätzliche Berechtigungskontrolle für die Verwaltung einer API aufgrund der sensiblen Natur der Ressourcenrichtlinie	Berechtigungsverwaltung	RestApi		
			RestApis		

Von Amazon-API-Gateway-Management definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Account	arn:${Partition}:apigateway:${Region}::/account	
ApiKey	arn:${Partition}:apigateway:${Region}::/apikeys/${ApiKeyId}	aws:ResourceTag/${TagKey}
ApiKeys	arn:${Partition}:apigateway:${Region}::/apikeys	aws:ResourceTag/${TagKey}
Authorizer	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/authorizers/${AuthorizerId}	apigateway:Request/AuthorizerType apigateway:Request/AuthorizerUri apigateway:Resource/AuthorizerType apigateway:Resource/AuthorizerUri aws:ResourceTag/${TagKey}
Authorizers	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/authorizers	apigateway:Request/AuthorizerType apigateway:Request/AuthorizerUri aws:ResourceTag/${TagKey}
BasePathMapping	arn:${Partition}:apigateway:${Region}::/domainnames/${DomainName}/basepathmappings/${BasePath}	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
BasePathMappings	arn:${Partition}:apigateway:${Region}::/domainnames/${DomainName}/basepathmappings	aws:ResourceTag/${TagKey}
ClientCertificate	arn:${Partition}:apigateway:${Region}::/clientcertificates/${ClientCertificateId}	aws:ResourceTag/${TagKey}
ClientCertificates	arn:${Partition}:apigateway:${Region}::/clientcertificates	aws:ResourceTag/${TagKey}
Deployment	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/deployments/${DeploymentId}	aws:ResourceTag/${TagKey}
Deployments	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/deployments	apigateway:Request/StageName aws:ResourceTag/${TagKey}
DocumentationPart	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/documentation/parts/${DocumentationPartId}	aws:ResourceTag/${TagKey}
DocumentationParts	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/documentation/parts	aws:ResourceTag/${TagKey}
DocumentationVersion	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/documentation/versions/${DocumentationVersionId}	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
DocumentationVersions	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/documentation/versions	aws:ResourceTag/${TagKey}
DomainName	arn:${Partition}:apigateway:${Region}::/domainnames/${DomainName}	apigateway:Request/EndpointType apigateway:Request/MtlsTrustStoreUri apigateway:Request/MtlsTrustStoreVersion apigateway:Request/SecurityPolicy apigateway:Resource/EndpointType apigateway:Resource/MtlsTrustStoreUri apigateway:Resource/MtlsTrustStoreVersion apigateway:Resource/SecurityPolicy aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
DomainNames	arn:${Partition}:apigateway:${Region}::/domainnames	apigateway:Request/EndpointType apigateway:Request/MtlsTrustStoreUri apigateway:Request/MtlsTrustStoreVersion apigateway:Request/SecurityPolicy aws:ResourceTag/${TagKey}
GatewayResponse	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/gatewayresponses/${ResponseType}	aws:ResourceTag/${TagKey}
GatewayResponses	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/gatewayresponses	aws:ResourceTag/${TagKey}
Integration	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/resources/${ResourceId}/methods/${HttpMethodType}/integration	aws:ResourceTag/${TagKey}
IntegrationResponse	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/resources/${ResourceId}/methods/${HttpMethodType}/integration/responses/${StatusCode}	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
Method	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/resources/${ResourceId}/methods/${HttpMethodType}	apigateway:Request/ApiKeyRequired apigateway:Request/RouteAuthorizationType apigateway:Resource/ApiKeyRequired apigateway:Resource/RouteAuthorizationType aws:ResourceTag/${TagKey}
MethodResponse	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/resources/${ResourceId}/methods/${HttpMethodType}/responses/${StatusCode}	aws:ResourceTag/${TagKey}
Model	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/models/${ModelName}	aws:ResourceTag/${TagKey}
Models	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/models	aws:ResourceTag/${TagKey}
RequestValidator	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/requestvalidators/${RequestValidatorId}	aws:ResourceTag/${TagKey}
RequestValidators	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/requestvalidators	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
Resource	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/resources/${ResourceId}	aws:ResourceTag/${TagKey}
Resources	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/resources	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
RestApi	`arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}`	apigateway:Request/ApiKeyRequired apigateway:Request/ApiName apigateway:Request/AuthorizerType apigateway:Request/AuthorizerUri apigateway:Request/DisableExecuteApiEndpoint apigateway:Request/EndpointType apigateway:Request/RouteAuthorizationType apigateway:Resource/ApiKeyRequired apigateway:Resource/ApiName apigateway:Resource/AuthorizerType apigateway:Resource/AuthorizerUri

Ressourcentypen	ARN	Bedingungsschlüssel
		apigateway:Resource/DisableExecuteApiEndpoint apigateway:Resource/EndpointType apigateway:Resource/RouteAuthorizationType aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
RestApis	arn:${Partition}:apigateway:${Region}::/restapis	apigateway:Request/ApiKeyRequired apigateway:Request/ApiName apigateway:Request/AuthorizerType apigateway:Request/AuthorizerUri apigateway:Request/DisableExecuteApiEndpoint apigateway:Request/EndpointType apigateway:Request/RouteAuthorizationType aws:ResourceTag/${TagKey}
Sdk	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/stages/${StageName}/sdks/${SdkType}	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
Stage	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/stages/${StageName}	apigateway:Request/AccessLoggingDestination apigateway:Request/AccessLoggingFormat apigateway:Resource/AccessLoggingDestination apigateway:Resource/AccessLoggingFormat aws:ResourceTag/${TagKey}
Stages	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/stages	apigateway:Request/AccessLoggingDestination apigateway:Request/AccessLoggingFormat aws:ResourceTag/${TagKey}
Template	arn:${Partition}:apigateway:${Region}::/restapis/models/${ModelName}/template	aws:ResourceTag/${TagKey}
UsagePlan	arn:${Partition}:apigateway:${Region}::/usageplans/${UsagePlanId}	aws:ResourceTag/${TagKey}
UsagePlans	arn:${Partition}:apigateway:${Region}::/usageplans	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
UsagePlanKey	arn:${Partition}:apigateway:${Region}::/usageplans/${UsagePlanId}/keys/${Id}	aws:ResourceTag/${TagKey}
UsagePlanKeys	arn:${Partition}:apigateway:${Region}::/usageplans/${UsagePlanId}/keys	aws:ResourceTag/${TagKey}
VpcLink	arn:${Partition}:apigateway:${Region}::/vpclinks/${VpcLinkId}	aws:ResourceTag/${TagKey}
VpcLinks	arn:${Partition}:apigateway:${Region}::/vpclinks	aws:ResourceTag/${TagKey}
Tags	arn:${Partition}:apigateway:${Region}::/tags/${UrlEncodedResourceARN}	

Bedingungsschlüssel für Amazon-API-Gateway-Management

Amazon-API-Gateway-Management definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
apigateway:Request/AccessLoggingDestination	Filtert den Zugriff nach Zugriffsprotokoll-Ziel Während der UpdateStage Operationen CreateStage und verfügbar	String

Bedingungsschlüssel	Beschreibung	Typ
apigateway:Request/AccessLoggingFormat	Filtert den Zugriff nach Zugriffsprotokollformat. Während der UpdateStage Operationen CreateStage und verfügbar	String
apigateway:Request/ApiKeyRequired	Filtert den Zugriff danach, ob ein API-Schlüssel erforderlich ist oder nicht. Verfügbar während der PutMethod Operationen CreateMethod und. Auch als Sammlung beim Import und Reimport erhältlich	ArrayOfBool
apigateway:Request/ApiName	Filtert den Zugriff nach API-Namen. Während der UpdateRestApi Operationen CreateRestApi und verfügbar	String
apigateway:Request/AuthorizerType	Filtert den Zugriff nach Berechtigungstyp in der Anfrage, zum Beispiel TOKEN, REQUEST, JWT. Verfügbar während CreateAuthorizer und UpdateAuthorizer. Auch während des Imports und Reimports verfügbar als ArrayOfString	ArrayOfString
apigateway:Request/AuthorizerUri	Filtert den Zugriff nach URI einer Lambda-Authorizer-Funktion. Verfügbar während CreateAuthorizer und. UpdateAuthorizer Auch während des Imports und Reimports verfügbar als ArrayOfString	ArrayOfString
apigateway:Request/DisableExecuteApiEndpoint	Filtert den Zugriff nach Status des standardmäßigen Execute-API-Endpunkts. Verfügbar während der Operationen CreateRestApi und DeleteRestApi	Bool
apigateway:Request/EndpointType	Filtert den Zugriff nach Endpunkttyp. Verfügbar während der UpdateRestApi Operationen CreateDomainName UpdateDomainName CreateRestApi,, und	ArrayOfString

Bedingungsschlüssel	Beschreibung	Typ
apigateway:Request/MtlsTrustStoreUri	Filtert den Zugriff nach URI des Truststores, der für die gegenseitige TLS-Authentifizierung verwendet wird. Verfügbar während der UpdateDomainName Operationen CreateDomainName und	String
apigateway:Request/MtlsTrustStoreVersion	Filtert den Zugriff nach Version des Truststores, der für die gegenseitige TLS-Authentifizierung verwendet wird. Während der UpdateDomainName Operationen CreateDomainName und verfügbar	String
apigateway:Request/RouteAuthorizationType	Filtert den Zugriff nach Berechtigungsart, zum Beispiel NONE, AWS_IAM, CUSTOM, JWT, COGNITO_USER_POOLS. Während der PutMethod Operationen CreateMethod und verfügbar Auch als Sammlung während des Imports verfügbar	ArrayOfString
apigateway:Request/SecurityPolicy	Filtert den Zugriff nach TLS-Version. Verfügbar während der UpdateDomain Operationen CreateDomain und	ArrayOfString
apigateway:Request/StageName	Filtert den Zugriff nach dem Namen der Bereitstellung, die Sie erstellen möchten. Während der CreateDeployment Operation verfügbar	String
apigateway:Resource/AccessLoggingDestination	Filtert den Zugriff nach Zugriffsprotokoll-Ziel der aktuellen Stage-Ressource. Verfügbar während UpdateStage der DeleteStage Operationen	String
apigateway:Resource/AccessLoggingFormat	Filtert den Zugriff nach Zugriffsprotokollformat der aktuellen Stage-Ressource. Während der DeleteStage Operationen UpdateStage und verfügbar	String

Bedingungsschlüssel	Beschreibung	Typ
apigateway:Resource/ApiKeyRequired	Filtert den Zugriff danach, ob ein API-Schlüssel für die vorhandene Methodenressource erforderlich ist oder nicht. Verfügbar während der DeleteMethod Operationen PutMethod und. Auch als Sammlung beim Reimport erhältlich	ArrayOfBool
apigateway:Resource/ApiName	Filtert den Zugriff nach dem API-Namen der vorhandenen RestApi Ressource. Verfügbar während UpdateRestApi und während des DeleteRestApi Betriebs	String
apigateway:Resource/AuthorizerType	Filtert den Zugriff nach dem aktuellen Berechtigungstyp, zum Beispiel TOKEN, REQUEST, JWT. Verfügbar während UpdateAuthorizer und während des DeleteAuthorizer Betriebs. Auch während des Reimports verfügbar als ArrayOfString	ArrayOfString
apigateway:Resource/AuthorizerUri	Filtert den Zugriff nach URI einer Lambda-Authorizer-Funktion. Verfügbar während UpdateAuthorizer und während des DeleteAuthorizer Betriebs. Auch während des Reimports verfügbar als ArrayOfString	ArrayOfString
apigateway:Resource/DisableExecuteApiEndpoint	Filtert den Zugriff nach dem Status des Standard-Execute-API-Endpunkts der aktuellen Ressource. RestApi Verfügbar während und während des Betriebs UpdateRestApi DeleteRestApi	Bool
apigateway:Resource/EndpointType	Filtert den Zugriff nach Endpunkttyp. Verfügbar während der DeleteRestApi Operationen UpdateDomainName DeleteDomainName UpdateRestApi,, und	ArrayOfString
apigateway:Resource/MtlsTrustStoreUri	Filtert den Zugriff nach URI des Truststores, der für die gegenseitige TLS-Authentifizierung verwendet wird. Verfügbar während UpdateDomainName und während des DeleteDomainName Betriebs	String

Bedingungsschlüssel	Beschreibung	Typ
apigateway:Resource/MtlsTrustStoreVersion	Filtert den Zugriff nach Version des Truststores, der für die gegenseitige TLS-Authentifizierung verwendet wird. Verfügbar während UpdateDomainName und während des DeleteDomainName Betriebs	String
apigateway:Resource/RouteAuthorizationType	Filtert den Zugriff nach Berechtigungstyp der vorhandenen Methodenressource, zum Beispiel NONE, AWS_IAM, CUSTOM, JWT, COGNITO_USER_POOLS. Verfügbar während der DeleteMethod Operationen PutMethod und. Auch als Sammlung beim Reimport erhältlich	ArrayOfString
apigateway:Resource/SecurityPolicy	Filtert den Zugriff nach TLS-Version. Verfügbar während UpdateDomain und während des DeleteDomain Betriebs	ArrayOfString
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tag-Schlüssel-Wert-Paare in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff über die Tags, die an die Ressource angehängt sind.	String
aws:TagKeys	Filtert Aktionen nach den Tag-Schlüsseln in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon-API-Gateway-Management V2

Amazon API Gateway Management V2 (Servicepräfix: `apigateway`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.

- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon-API-Gateway-Management V2 definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DELETE	Gewährt die Berechtigung zum Löschen einer bestimmten Ressource	Write	AccessLogSettings		
			Api		
			ApiMapping		
			Authorizer		
			AuthorizersCache		
			Cors		
			Deployment		
			Integration		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			IntegrationResponse		
			Model		
			Route		
			RouteRequestParameter		
			RouteResponse		
			RouteSettings		
			Stage		
			VpcLink		
				aws:RequestTag/${TagKey} aws:TagKeys	
GET	Gewährt die Berechtigung zum Lesen einer bestimmten Ressource	Read	AccessLogSettings		
			Api		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			ApiMapping		
			ApiMappings		
			Apis		
			Authorizer		
			Authorizers		
			AuthorizersCache		
			Cors		
			Deployment		
			Deployments		
			ExportedAPI		
			Integration		
			IntegrationResponse		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			IntegrationResponses		
			Integrations		
			Model		
			ModelTemplate		
			Models		
			Route		
			RouteRequestParameter		
			RouteResponse		
			RouteResponses		
			RouteSettings		
			Routes		
			Stage		
			Stages		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			VpcLink		
			VpcLinks		
PATCH	Gewährt die Berechtigung zum Aktualisieren einer bestimmten Ressource	Write	Api		
			ApiMapping		
			Authorizer		
			Deployment		
			Integration		
			IntegrationResponse		
			Model		
			Route		
			RouteRequestParameter		
			RouteResponse		
			Stage		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			VpcLink		
				aws:RequestTag/${TagKey} aws:TagKeys	
POST	Gewährt die Berechtigung zum Erstellen einer bestimmten Ressource	Write	ApiMappings		
			Apis		
			Authorizers		
			Deployments		
			IntegrationResponses		
			Integrations		
			Models		
			RouteResponses		
			Routes		
			Stages		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			VpcLinks		
				aws:RequestTag/${TagKey} aws:TagKeys	
PUT	Gewährt die Berechtigung zum Aktualisieren einer bestimmten Ressource	Write	Api		
			Apis		
				aws:RequestTag/${TagKey} aws:TagKeys	

Von Amazon-API-Gateway-Management V2 definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
AccessLogSettings	`arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/stages/${StageName}/accesslogsettings`	aws:ResourceTag/${TagKey}
Api	`arn:${Partition}:apigateway:${Region}::/apis/${ApiId}`	apigateway:Request/ApiKeyRequired apigateway:Request/ApiName apigateway:Request/AuthorizerType apigateway:Request/AuthorizerUri apigateway:Request/DisableExecuteApiEndpoint apigateway:Request/EndpointType apigateway:Request/RouteAuthorizationType apigateway:Resource/ApiKeyRequired apigateway:Resource/ApiName apigateway:Resource/AuthorizerType

Ressourcentypen	ARN	Bedingungsschlüssel
		apigateway:Resource/AuthorizerUri apigateway:Resource/DisableExecuteApiEndpoint apigateway:Resource/EndpointType apigateway:Resource/RouteAuthorizationType aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
Apis	arn:${Partition}:apigateway:${Region}::/apis	apigateway:Request/ApiKeyRequired apigateway:Request/ApiName apigateway:Request/AuthorizerType apigateway:Request/AuthorizerUri apigateway:Request/DisableExecuteApiEndpoint apigateway:Request/EndpointType apigateway:Request/RouteAuthorizationType aws:ResourceTag/${TagKey}
ApiMapping	arn:${Partition}:apigateway:${Region}::/domainnames/${DomainName}/apimappings/${ApiMappingId}	aws:ResourceTag/${TagKey}
ApiMappings	arn:${Partition}:apigateway:${Region}::/domainnames/${DomainName}/apimappings	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
Authorizer	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/authorizers/${AuthorizerId}	apigateway:Request/AuthorizerType apigateway:Request/AuthorizerUri apigateway:Resource/AuthorizerType apigateway:Resource/AuthorizerUri aws:ResourceTag/${TagKey}
Authorizers	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/authorizers	apigateway:Request/AuthorizerType apigateway:Request/AuthorizerUri aws:ResourceTag/${TagKey}
AuthorizersCache	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/stages/${StageName}/cache/authorizers	aws:ResourceTag/${TagKey}
Cors	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/cors	aws:ResourceTag/${TagKey}
Deployment	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/deployments/${DeploymentId}	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
Deployments	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/deployments	apigateway:Request/StageName aws:ResourceTag/${TagKey}
ExportedAPI	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/exports/${Specification}	aws:ResourceTag/${TagKey}
Integration	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/integrations/${IntegrationId}	aws:ResourceTag/${TagKey}
Integrations	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/integrations	aws:ResourceTag/${TagKey}
IntegrationResponse	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/integrations/${IntegrationId}/integrationresponses/${IntegrationResponseId}	aws:ResourceTag/${TagKey}
IntegrationResponses	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/integrations/${IntegrationId}/integrationresponses	aws:ResourceTag/${TagKey}
Model	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/models/${ModelId}	aws:ResourceTag/${TagKey}
Models	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/models	aws:ResourceTag/${TagKey}
ModelTemplate	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/models/${ModelId}/template	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
Route	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/routes/${RouteId}	apigateway:Request/ApiKeyRequired apigateway:Request/RouteAuthorizationType apigateway:Resource/ApiKeyRequired apigateway:Resource/RouteAuthorizationType aws:ResourceTag/${TagKey}
Routes	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/routes	apigateway:Request/ApiKeyRequired apigateway:Request/RouteAuthorizationType aws:ResourceTag/${TagKey}
RouteResponse	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/routes/${RouteId}/routeresponses/${RouteResponseId}	aws:ResourceTag/${TagKey}
RouteResponses	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/routes/${RouteId}/routeresponses	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
RouteRequestParameter	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/routes/${RouteId}/requestparameters/${RequestParameterKey}	aws:ResourceTag/${TagKey}
RouteSettings	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/stages/${StageName}/routesettings/${RouteKey}	aws:ResourceTag/${TagKey}
Stage	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/stages/${StageName}	apigateway:Request/AccessLoggingDestination apigateway:Request/AccessLoggingFormat apigateway:Resource/AccessLoggingDestination apigateway:Resource/AccessLoggingFormat aws:ResourceTag/${TagKey}
Stages	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/stages	apigateway:Request/AccessLoggingDestination apigateway:Request/AccessLoggingFormat aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
VpcLink	`arn:${Partition}:apigateway:${Region}::/vpclinks/${VpcLinkId}`	aws:ResourceTag/${TagKey}
VpcLinks	`arn:${Partition}:apigateway:${Region}::/vpclinks`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon-API-Gateway-Management V2

Amazon API Gateway Management V2 definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
apigateway:Request/AccessLoggingDestination	Filtert den Zugriff nach Zugriffsprotokoll-Ziel Verfügbar während CreateStage der UpdateStage Operationen	String
apigateway:Request/AccessLoggingFormat	Filtert den Zugriff nach Zugriffsprotokollformat. Während der UpdateStage Operationen CreateStage und verfügbar	String
apigateway:Request/ApiKeyRequired	Filtert den Zugriff nach API-Anforderung. Verfügbar während der UpdateRoute Operationen CreateRoute und. Auch als Sammlung beim Import und Reimport erhältlich	ArrayOfBool

Bedingungsschlüssel	Beschreibung	Typ
apigateway:Request/ApiName	Filtert den Zugriff nach API-Namen. Während der UpdateApi Operationen CreateApi und verfügbar	String
apigateway:Request/AuthorizerType	Filtert den Zugriff nach Berechtigungstyp in der Anfrage, zum Beispiel REQUEST oder JWT. Verfügbar während CreateAuthorizer und UpdateAuthorizer. Auch während des Imports und Reimports verfügbar als ArrayOfString	ArrayOfString
apigateway:Request/AuthorizerUri	Filtert den Zugriff nach URI einer Lambda-Authorizer-Funktion. Verfügbar während CreateAuthorizer und. UpdateAuthorizer Auch während des Imports und Reimports verfügbar als ArrayOfString	ArrayOfString
apigateway:Request/DisableExecuteApiEndpoint	Filtert den Zugriff nach Status des standardmäßigen Execute-API-Endpunkts. Verfügbar während der Operationen CreateApi und UpdateApi	Bool
apigateway:Request/EndpointType	Filtert den Zugriff nach Endpunkttyp. Verfügbar während der UpdateApi Operationen CreateDomainName UpdateDomainName CreateApi,, und	ArrayOfString
apigateway:Request/MtlsTrustStoreUri	Filtert den Zugriff nach URI des Truststores, der für die gegenseitige TLS-Authentifizierung verwendet wird. Verfügbar während der UpdateDomainName Operationen CreateDomainName und	String
apigateway:Request/MtlsTrustStoreVersion	Filtert den Zugriff nach Version des Truststores, der für die gegenseitige TLS-Authentifizierung verwendet wird. Während der UpdateDomainName Operationen CreateDomainName und verfügbar	String

Bedingungsschlüssel	Beschreibung	Typ
apigateway:Request/RouteAuthorizationType	Filtert den Zugriff nach Berechtigungstyp, zum Beispiel NONE, AWS_IAM, CUSTOM, JWT. Verfügbar während der UpdateRoute Operationen CreateRoute und. Auch als Sammlung beim Import erhältlich	ArrayOfString
apigateway:Request/SecurityPolicy	Filtert den Zugriff nach TLS-Version. Während der UpdateDomain Operationen CreateDomain und verfügbar	ArrayOfString
apigateway:Request/StageName	Filtert den Zugriff nach dem Namen der Bereitstellung, die Sie erstellen möchten. Während der CreateDeployment Operation verfügbar	String
apigateway:Resource/AccessLoggingDestination	Filtert den Zugriff nach Zugriffsprotokoll-Ziel der aktuellen Stage-Ressource. Verfügbar während UpdateStage der DeleteStage Operationen	String
apigateway:Resource/AccessLoggingFormat	Filtert den Zugriff nach Zugriffsprotokollformat der aktuellen Stage-Ressource. Während der DeleteStage Operationen UpdateStage und verfügbar	String
apigateway:Resource/ApiKeyRequired	Filtert den Zugriff nach Anforderung eines API-Schlüssels für die vorhandene Route-Ressource. Verfügbar während der DeleteRoute Operationen UpdateRoute und. Auch als Sammlung beim Reimport erhältlich	ArrayOfBool
apigateway:Resource/ApiName	Filtert den Zugriff nach API-Namen. Während der DeleteApi Operationen UpdateApi und verfügbar	String

Bedingungsschlüssel	Beschreibung	Typ
apigateway:Resource/AuthorizerType	Filtert den Zugriff nach dem aktuellen Berechtigungstyp, zum Beispiel REQUEST oder JWT. Verfügbar während UpdateAuthorizer und während des DeleteAuthorizer Betriebs. Auch während des Imports und Reimports verfügbar als ArrayOfString	ArrayOfString
apigateway:Resource/AuthorizerUri	Filtert den Zugriff nach dem URI des aktuellen Lambda-Authorizers, der mit der aktuellen API verknüpft ist. Verfügbar während UpdateAuthorizer und. DeleteAuthorizer Auch als Sammlung beim Reimport erhältlich	ArrayOfString
apigateway:Resource/DisableExecuteApiEndpoint	Filtert den Zugriff nach Status des standardmäßigen Execute-API-Endpunkts. Verfügbar während der DeleteApi Operationen UpdateApi und	Bool
apigateway:Resource/EndpointType	Filtert den Zugriff nach Endpunkttyp. Verfügbar während der DeleteApi Operationen UpdateDomainName DeleteDomainName UpdateApi,, und	ArrayOfString
apigateway:Resource/MtlsTrustStoreUri	Filtert den Zugriff nach URI des Truststores, der für die gegenseitige TLS-Authentifizierung verwendet wird. Verfügbar während der DeleteDomainName Operationen UpdateDomainName und	String
apigateway:Resource/MtlsTrustStoreVersion	Filtert den Zugriff nach Version des Truststores, der für die gegenseitige TLS-Authentifizierung verwendet wird. Während der DeleteDomainName Operationen UpdateDomainName und verfügbar	String

Bedingungsschlüssel	Beschreibung	Typ
apigateway:Resource/RouteAuthorizationType	Filtert den Zugriff nach Berechtigungstyp der vorhandenen Routenressource, zum Beispiel NONE, AWS_IAM, CUSTOM. Verfügbar während der DeleteRoute Operationen UpdateRoute und. Auch als Sammlung beim Reimport erhältlich	ArrayOfString
apigateway:Resource/SecurityPolicy	Filtert den Zugriff nach TLS-Version. Während der DeleteDomainName Operationen UpdateDomainName und verfügbar	ArrayOfString
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	String
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS App Mesh

AWS App Mesh (Dienstpräfix:`appmesh`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS App Mesh definierte Aktionen

- Von AWS App Mesh definierte Ressourcentypen
- Bedingungsschlüssel für AWS App Mesh

Von AWS App Mesh definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateGatewayRoute	Gewährt die Berechtigung zum Erstellen einer Gateway-Route, die mit einem virtuellen Gateway verknüpft ist	Write	gatewayRoute*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualService		
CreateMesh	Gewährt die Berechtigung zum Erstellen eines Service-Mesh	Write	mesh*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRoute	Gewährt die Berechtigung zum Erstellen einer Route, die mit einem virtuellen Router verknüpft ist	Write	route*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualNode		
CreateVirtualGateway	Gewährt die Berechtigung zum Erstellen eines virtuelle	Write	virtualGateway*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	n Gateways innerhalb eines Service-Mesh			aws:TagKeys aws:RequestTag/${TagKey}	
CreateVirtualNode	Gewährt die Berechtigung zum Erstellen eines virtuellen Knotens innerhalb eines Service-Mesh	Write	virtualNode*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualService		
CreateVirtualRouter	Gewährt die Berechtigung zum Erstellen eines virtuellen Routers in einem Service-Mesh	Write	virtualRouter*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateVirtualService	Gewährt die Berechtigung zum Erstellen eines virtuellen Services innerhalb eines Service-Mesh	Write	virtualService*	aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			virtualNode		
			virtualRouter		
DeleteGatewayRoute	Gewährt die Berechtigung zum Löschen einer bestehenden Gateway-Route	Write	gatewayRoute*		
DeleteMesh	Gewährt die Berechtigung zum Löschen eines bestehenden Service-Mesh	Schreiben	mesh*		
DeleteMeshPolicy [nur Berechtigung]	Erteilt die Berechtigung zum Löschen der RAM-Zugriffskontrollrichtlinie für ein Mesh	Schreiben	mesh*		
DeleteRoute	Gewährt die Berechtigung zum Löschen einer bestehenden Route	Write	route*		
DeleteVirtualGateway	Gewährt die Berechtigung zum Löschen eines vorhandenen virtuellen Gateways	Write	virtualGateway*		
DeleteVirtualNode	Gewährt die Berechtigung zum Löschen eines bestehenden virtuellen Knotens	Write	virtualNode*		
DeleteVirtualRouter	Gewährt die Berechtigung zum Löschen eines vorhandenen virtuellen Routers	Write	virtualRouter*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteVirtualService	Gewährt die Berechtigung zum Löschen eines vorhandenen virtuellen Services	Write	virtualService*		
DescribeGatewayRoute	Gewährt die Berechtigung zum Beschreiben einer vorhandenen Gatewayroute	Read	gatewayRoute*		
DescribeMesh	Gewährt die Berechtigung zum Beschreiben eines vorhandenen Service-Mesh	Read	mesh*		
DescribeRoute	Gewährt die Berechtigung zum Beschreiben einer vorhandenen Route	Read	route*		
DescribeVirtualGateway	Gewährt die Berechtigung zur Beschreibung eines vorhandenen virtuellen Gateways	Read	virtualGateway*		
DescribeVirtualNode	Gewährt die Berechtigung zum Beschreiben eines vorhandenen virtuellen Knotens	Read	virtualNode*		
DescribeVirtualRouter	Gewährt die Berechtigung, einen bestehenden virtuellen Router zu beschreiben	Read	virtualRouter*		
DescribeVirtualService	Gewährt die Berechtigung, einen bestehenden virtuellen Service zu beschreiben	Lesen	virtualService*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetMeshPolicy [nur Berechtigung]	Erteilt die Berechtigung zum Lesen der RAM-Zugriffskontrollrichtlinie für ein Mesh	Lesen	mesh*		
ListGatewayRoutes	Gewährt die Berechtigung zum Auflisten vorhandener Gateway-Routen in einem Service-Mesh	List	virtualGateway*		
ListMeshes	Gewährt die Berechtigung zum Auflisten vorhandener Service-Meshes	List			
ListRoutes	Gewährt die Berechtigung zum Auflisten vorhandener Routen in einem Service-Mesh	List	virtualRouter*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für eine App-Mesh-Ressource	List	gatewayRoute		
			mesh		
			route		
			virtualGateway		
			virtualNode		
			virtualRouter		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			virtualService		
ListVirtualGateways	Gewährt die Berechtigung zum Auflisten vorhandener virtueller Gateways in einem Service-Mesh	List	mesh*		
ListVirtualNodes	Gewährt die Berechtigung zum Auflisten vorhandener virtueller Knoten	List	mesh*		
ListVirtualRouters	Gewährt die Berechtigung zum Auflisten vorhandener virtueller Router in einem Service-Mesh	List	mesh*		
ListVirtualServices	Gewährt die Berechtigung zum Auflisten vorhandener virtueller Services in einem Service-Mesh	Auflisten	mesh*		
PutMeshPolicy [nur Berechtigung]	Erteilt die Berechtigung, die RAM-Zugriffskontrollrichtlinie für ein Mesh zu definieren	Schreiben	mesh*		
StreamAggregatedResources	Erteilt die Erlaubnis, gestreamte Ressourcen für einen App Mesh Mesh-Endpunkt zu empfangen (VirtualNode/VirtualGateway)	Lesen	virtualGateway		
			virtualNode		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung, eine Ressource mit einem bestimmten resourceArn zu markieren	Tagging	gatewayRoute		
			mesh		
			route		
			virtualGateway		
			virtualNode		
			virtualRouter		
			virtualService		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen eines Tags von einer Ressource	Tagging	gatewayRoute		
			mesh		
			route		
			virtualGateway		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			virtualNode		
			virtualRouter		
			virtualService		
				aws:TagKeys	
UpdateGatewayRoute	Gewährt die Berechtigung zum Aktualisieren einer vorhandenen Gateway-Route für ein bestimmtes Service-Mesh und virtuelles Gateway	Write	gatewayRoute*		
			virtualService		
UpdateMesh	Gewährt die Berechtigung zum Aktualisieren eines vorhandenen Service-Mesh	Write	mesh*		
UpdateRoute	Gewährt die Berechtigung zum Aktualisieren einer vorhandenen Route für ein bestimmtes Service-Mesh und einen virtuellen Router	Write	route*		
			virtualNode		
UpdateVirtualGateway	Gewährt die Berechtigung zum Aktualisieren eines vorhandenen virtuellen Gateways in einem bestimmten Service-Mesh	Write	virtualGateway*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateVirtualNode	Gewährt die Berechtigung zum Aktualisieren eines vorhandenen virtuellen Knotens in einem bestimmten Service-Mesh	Write	virtualNode*		
UpdateVirtualRouter	Gewährt die Berechtigung zum Aktualisieren eines vorhandenen virtuellen Routers in einem bestimmten Service-Mesh	Write	virtualRouter*		
UpdateVirtualService	Gewährt die Berechtigung zum Aktualisieren eines vorhandenen virtuellen Services in einem angegebenen Service-Mesh	Write	virtualService*		
			virtualNode		
			virtualRouter		

Von AWS App Mesh definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
mesh	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}`	aws:ResourceTag/${TagKey}
virtualService	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualService/${VirtualServiceName}`	aws:ResourceTag/${TagKey}
virtualNode	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualNode/${VirtualNodeName}`	aws:ResourceTag/${TagKey}
virtualRouter	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}`	aws:ResourceTag/${TagKey}
route	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}/route/${RouteName}`	aws:ResourceTag/${TagKey}
virtualGateway	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualGateway/${VirtualGatewayName}`	aws:ResourceTag/${TagKey}
gatewayRoute	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualGateway/${VirtualGatewayName}/gatewayRoute/${GatewayRouteName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS App Mesh

AWS App Mesh definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen

zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen durch das Vorhandensein von Tag-Schlüssel-Werte-Paaren in der Anforderung.	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen durch Tag-Schlüssel-Werte-Paare, die der Ressource zugeordnet sind	Zeichenfolge
aws:TagKeys	Filtert Aktionen durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS App Mesh Preview

AWS App Mesh Preview (Dienstpräfix:`appmesh-preview`) bietet die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS App Mesh Preview definierte Aktionen
- Von AWS App Mesh Preview definierte Ressourcentypen

- Bedingungsschlüssel für AWS App Mesh Preview

Von AWS App Mesh Preview definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateGatewayRoute	Gewährt die Berechtigung zum Erstellen einer Gateway-Route, die mit einem virtuellen Gateway verknüpft ist	Write	gatewayRoute*		
			virtualService		
CreateMesh	Gewährt die Berechtigung zum Erstellen eines Service-Mesh	Write	mesh*		
CreateRoute	Gewährt die Berechtigung zum Erstellen einer Route, die mit einem virtuellen Router verknüpft ist	Write	route*		
			virtualNode		
CreateVirtualGateway	Gewährt die Berechtigung zum Erstellen eines virtuellen Gateways innerhalb eines Service-Mesh	Write	virtualGateway*		
CreateVirtualNode	Gewährt die Berechtigung zum Erstellen eines virtuellen Knotens innerhalb eines Service-Mesh	Write	virtualNode*		
			virtualService		
CreateVirtualRouter	Gewährt die Berechtigung zum Erstellen eines virtuellen Routers in einem Service-Mesh	Write	virtualRouter*		
CreateVirtualService	Gewährt die Berechtigung zum Erstellen eines virtuelle	Write	virtualService*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	n Services innerhalb eines Service-Mesh		virtualNode		
			virtualRouter		
DeleteGatewayRoute	Gewährt die Berechtigung zum Löschen einer bestehenden Gateway-Route	Write	gatewayRoute*		
DeleteMesh	Gewährt die Berechtigung zum Löschen eines bestehenden Service-Mesh	Schreiben	mesh*		
DeleteMeshPolicy [nur Berechtigung]	Erteilt die Berechtigung zum Löschen der RAM-Zugriffskontrollrichtlinie für ein Mesh	Schreiben	mesh*		
DeleteRoute	Gewährt die Berechtigung zum Löschen einer bestehenden Route	Write	route*		
DeleteVirtualGateway	Gewährt die Berechtigung zum Löschen eines vorhandenen virtuellen Gateways	Write	virtualGateway*		
DeleteVirtualNode	Gewährt die Berechtigung zum Löschen eines bestehenden virtuellen Knotens	Write	virtualNode*		
DeleteVirtualRouter	Gewährt die Berechtigung zum Löschen eines vorhandenen virtuellen Routers	Write	virtualRouter*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteVirtualService	Gewährt die Berechtigung zum Löschen eines vorhandenen virtuellen Services	Write	virtualService*		
DescribeGatewayRoute	Gewährt die Berechtigung zum Beschreiben einer vorhandenen Gatewayroute	Read	gatewayRoute*		
DescribeMesh	Gewährt die Berechtigung zum Beschreiben eines vorhandenen Service-Mesh	Read	mesh*		
DescribeRoute	Gewährt die Berechtigung zum Beschreiben einer vorhandenen Route	Read	route*		
DescribeVirtualGateway	Gewährt die Berechtigung zur Beschreibung eines vorhandenen virtuellen Gateways	Read	virtualGateway*		
DescribeVirtualNode	Gewährt die Berechtigung zum Beschreiben eines vorhandenen virtuellen Knotens	Read	virtualNode*		
DescribeVirtualRouter	Gewährt die Berechtigung, einen bestehenden virtuellen Router zu beschreiben	Read	virtualRouter*		
DescribeVirtualService	Gewährt die Berechtigung, einen bestehenden virtuellen Service zu beschreiben	Lesen	virtualService*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetMeshPolicy [nur Berechtigung]	Erteilt die Berechtigung zum Lesen der RAM-Zugriffskontrollrichtlinie für ein Mesh	Lesen	mesh*		
ListGatewayRoutes	Gewährt die Berechtigung zum Auflisten vorhandener Gateway-Routen in einem Service-Mesh	List	virtualGateway*		
ListMeshes	Gewährt die Berechtigung zum Auflisten vorhandener Service-Meshes	List			
ListRoutes	Gewährt die Berechtigung zum Auflisten vorhandener Routen in einem Service-Mesh	List	virtualRouter*		
ListVirtualGateways	Gewährt die Berechtigung zum Auflisten vorhandener virtueller Gateways in einem Service-Mesh	List	mesh*		
ListVirtualNodes	Gewährt die Berechtigung zum Auflisten vorhandener virtueller Knoten	List	mesh*		
ListVirtualRouters	Gewährt die Berechtigung zum Auflisten vorhandener virtueller Router in einem Service-Mesh	List	mesh*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListVirtualServices	Gewährt die Berechtigung zum Auflisten vorhandener virtueller Services in einem Service-Mesh	Auflisten	mesh*		
PutMeshPolicy [nur Berechtigung]	Erteilt die Berechtigung, die RAM-Zugriffskontrollrichtlinie für ein Mesh zu definieren	Schreiben	mesh*		
StreamAggregatedResources	Erteilt die Erlaubnis, gestreamte Ressourcen für einen App Mesh Mesh-Endpunkt zu empfangen (VirtualNode/VirtualGateway)	Lesen	virtualGateway		
			virtualNode		
UpdateGatewayRoute	Gewährt die Berechtigung zum Aktualisieren einer vorhandenen Gateway-Route für ein bestimmtes Service-Mesh und virtuelles Gateway	Write	gatewayRoute*		
			virtualService		
UpdateMesh	Gewährt die Berechtigung zum Aktualisieren eines vorhandenen Service-Mesh	Write	mesh*		
UpdateRoute	Gewährt die Berechtigung zum Aktualisieren einer vorhandenen Route für ein bestimmtes Service-Mesh und einen virtuellen Router	Write	route*		
			virtualNode		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateVirtualGateway	Gewährt die Berechtigung zum Aktualisieren eines vorhandenen virtuellen Gateways in einem bestimmten Service-Mesh	Write	virtualGateway*		
UpdateVirtualNode	Gewährt die Berechtigung zum Aktualisieren eines vorhandenen virtuellen Knotens in einem bestimmten Service-Mesh	Write	virtualNode*		
UpdateVirtualRouter	Gewährt die Berechtigung zum Aktualisieren eines vorhandenen virtuellen Routers in einem bestimmten Service-Mesh	Write	virtualRouter*		
UpdateVirtualService	Gewährt die Berechtigung zum Aktualisieren eines vorhandenen virtuellen Services in einem angegebenen Service-Mesh	Write	virtualService*		
			virtualNode		
			virtualRouter		

Von AWS App Mesh Preview definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
mesh	`arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}`	
virtualService	`arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualService/${VirtualServiceName}`	
virtualNode	`arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualNode/${VirtualNodeName}`	
virtualRouter	`arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}`	
route	`arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}/route/${RouteName}`	
virtualGateway	`arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualGateway/${VirtualGatewayName}`	
gatewayRoute	`arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualGateway/${VirtualGatewayName}/gatewayRoute/${GatewayRouteName}`	

Bedingungsschlüssel für AWS App Mesh Preview

App Mesh Preview besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS App Runner

AWS App Runner (Servicepräfix: `apprunner`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS App Runner definierte Aktionen
- Von AWS App Runner definierte Ressourcentypen
- Bedingungsschlüssel für AWS App Runner

Von AWS App Runner definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung

mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Associate CustomDomain	Gewährt die Berechtigung zum Verknüpfen Ihres eigenen Domainnamen mit der AWS-App-Runner-Subdomain-URL Ihres App-Runner-Services	Schreiben	service*		
Associate WebAcl [nur Berechtigung]	Gewährt die Berechtigung zum Zuordnen des Services mit einer AWS-WAF-Web-ACL	Schreiben	service* webacl*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAutoScalingConfiguration	Gewährt die Berechtigung zum Erstellen einer AWS-App-Runner-Auto-Scaling-Konfigurationsressource	Write	autoscalingconfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnection	Gewährt die Berechtigung zum Erstellen einer AWS-App-Runner-Verbindungsressource	Schreiben	connection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateObservabilityConfiguration	Gewährt die Berechtigung zum Erstellen einer AWS-App-Runner-Beobachtbarkeits-Konfigurationsressource	Schreiben	observabilityconfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateService		Schreiben	service*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Erteilt die Berechtigung zum Erstellen einer AWS-App-Runner-Service-Ressource		autoscalingconfiguration		
			connection		
			observabilityconfiguration		
			vpcconnector		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys apprunner:ConnectionArn apprunner:AutoScalingConfigurationArn apprunner:ObservabilityConfigurationArn apprunner:VpcConnectorArn	
CreateVpcConnector	Erteilt die Berechtigung zum Erstellen einer AWS-App-Runner VPC-Verbindungsressource	Schreiben	vpcconnector*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVpcIngressConnection	Gewährt die Berechtigung zum Erstellen einer AWS-App-Runner-VPC-Ingress-Verbindungsressource	Schreiben	vpcingressconnection*		
				aws:RequestTag/${TagKey} aws:TagKeys apprunner:ServiceArn apprunner:VpcId apprunner:VpcEndpointId	
DeleteAutoScalingConfiguration	Gewährt die Berechtigung zum Löschen einer AWS-App-Runner-Auto-Scaling-Konfigurationsressource	Schreiben	autoscalingconfiguration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteConnection	Erteilt die Berechtigung zum Löschen einer AWS-App-Runner-Verbindungsressource	Schreiben	connection*		
DeleteObservabilityConfiguration	Gewährt die Berechtigung zum Löschen einer AWS-App-Runner-Beobachtbarkeits-Konfigurationsressource	Schreiben	observabilityconfiguration*		
DeleteService	Erteilt die Berechtigung zum Löschen einer AWS-App-Runner-Service-Ressource	Schreiben	service*		
DeleteVpcConnector	Erteilt die Berechtigung zum Löschen einer AWS-App-Runner VPC-Verbindungsressource	Schreiben	vpcconnector*		
DeleteVpcIngressConnection	Gewährt die Berechtigung zum Löschen einer VPC-Ingress-Verbindungsressource von AWS App Runner	Schreiben	vpcingressconnection*		
DescribeAutoScalingConfiguration	Erteilt die Berechtigung zum Abrufen von Beschreibungen einer AWS-App-Runner-Auto-Scaling-Konfigurationsressource	Lesen	autoscalingconfiguration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeCustomDomains	Gewährt die Berechtigung zum Abrufen von Beschreibungen von benutzerdefinierten Domain-Namen im Zusammenhang mit einem AWS-App-Runner-Service	Lesen	service*		
DescribeObservabilityConfiguration	Erteilt die Berechtigung zum Abrufen von Beschreibungen einer AWS-App-Runner-Beobachtbarkeits-Konfigurationsressource	Lesen	observabilityconfiguration*		
DescribeOperation	Erteilt die Berechtigung zum Abrufen der Beschreibung eines Vorgangs, der in einem AWS-App-Runner-Service stattgefunden hat	Lesen	service*		
DescribeService	Erteilt die Berechtigung zum Abrufen der Beschreibung einer AWS-App-Runner-Service-Ressource	Lesen	service*		
DescribeVpcConnector	Erteilt die Berechtigung zum Abrufen von Beschreibungen einer AWS-App-Runner-VPC-Ressource	Lesen	vpcconnector*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeVpcIngressConnection	Gewährt die Berechtigung zum Abrufen einer Beschreibung einer VPC-Ingress-Verbindungsressource von AWS App Runner	Lesen	vpcingressconnection*		
DescribeWebAclForService [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen der AWS-WAF-Web-ACL, die einem AWS-App-Runner-Service zugeordnet ist	Lesen	service*		
DisassociateCustomDomain	Gewährt die Berechtigung, einen benutzerdefinierten Domainnamen von einem AWS-App-Runner-Service zu trennen	Schreiben	service*		
DisassociateWebAcl [nur Berechtigung]	Gewährt die Berechtigung zum Aufheben der Zuordnung des Services zu einer AWS-WAF-Web-ACL	Schreiben	service*		
ListAssociatedServicesForWebAcl [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der Services, die einer AWS-WAF-Web-ACL zugeordnet sind	Auflisten	webacl*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAutoScalingConfigurations	Gewährt die Berechtigung zum Abrufen einer Liste der Auto-Scaling-Konfigurationen von AWS App Runner in Ihrem AWS-Konto	Auflisten			
ListConnections	Erteilt die Berechtigung zum Abrufen einer Liste von AWS-App-Runner-Verbindungen in Ihrem AWS-Konto	Auflisten			
ListObservabilityConfigurations	Erteilt die Berechtigung zum Abrufen einer Liste von AWS-App-Runner-Beobachtbarkeitskonfigurationen in Ihrem AWS-Konto	Auflisten			
ListOperations	Erteilt die Berechtigung zum Abrufen einer Liste von Vorgängen, die bei einer AWS-App-Runner-Service-Ressource stattgefunden haben	Auflisten	service*		
ListServices	Gewährt die Berechtigung zum Abrufen einer Liste der laufenden AWS-App-Runner-Services in Ihrem AWS-Konto	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListServicesForAutoScalingConfiguration	Gewährt die Berechtigung zum Abrufen einer Liste der zugehörigen AWS AppRunner-Services einer automatischen Skalierungskonfiguration von App Runner in Ihrem AWS-Konto	Auflisten	autoscalingconfiguration*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags, die mit einer AWS-App-Runner-Ressource verknüpft sind	Lesen	autoscalingconfiguration		
			connection		
			observabilityconfiguration		
			service		
			vpcconnector		
ListVpcConnectors	Erteilt die Berechtigung zum Abrufen einer Liste der AWS-App-Runner VPC-Verbindungen in Ihrem AWS-Konto	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListVpcIngressConnections	Gewährt die Berechtigung zum Aktualisieren einer VPC-Ingress-Verbindungsressource von AWS App Runner in Ihrem AWS-Konto	Auflisten			
PauseService	Gewährt die Berechtigung zum Pausieren eines aktiven AWS-App-Runner-Services	Write	service*		
ResumeService	Gewährt die Erlaubnis zum Fortsetzen eines aktiven AWS-App-Runner-Services	Write	service*		
StartDeployment	Gewährt die Erlaubnis zum Initiieren einer manuellen Bereitstellung für einen AWS-App-Runner-Service	Write	service*		
TagResource	Erteilt die Berechtigung zum Hinzufügen von Tags zu oder zum Aktualisieren von Tagwerten einer AWS-App-Runner-Ressource	Markieren	autoscalingconfiguration		
			connection		
			observabilityconfiguration		
			service		
			vpcconnector		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			vpcingressconnection		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Erteilt die Berechtigung zum Entfernen von Tags aus einer AWS-App-Runner-Ressource	Markierung	autoscalingconfiguration		
			connection		
			observabilityconfiguration		
			service		
			vpcconnector		
			vpcingressconnection		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateDefaultAutoScalingConfiguration	Gewährt die Berechtigung zum Aktualisieren einer automatischen Skalierungskonfiguration von AWS App Runner, um die Standardkonfiguration in Ihrem AWS-Konto zu sein	Schreiben	autoscalingconfiguration*		
UpdateService	Erteilt die Berechtigung zum Aktualisieren einer AWS-App-Runner-Service-Ressource	Schreiben	service*		
			autoscalingconfiguration		
			connection		
			observabilityconfiguration		
			vpcconnector		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				apprunner:ConnectionArn apprunner:AutoScalingConfigurationArn apprunner:ObservabilityConfigurationArn apprunner:VpcConnectorArn	
UpdateVpcIngressConnection	Gewährt die Berechtigung zum Aktualisieren einer VPC-Ingress-Verbindungsressource von AWS App Runner	Schreiben	vpcingressconnection*		
				apprunner:VpcId apprunner:VpcEndpointId	

Von AWS App Runner definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
service	`arn:${Partition}:apprunner:${Region}:${Account}:service/${ServiceName}/${ServiceId}`	aws:ResourceTag/${TagKey}
connection	`arn:${Partition}:apprunner:${Region}:${Account}:connection/${ConnectionName}/${ConnectionId}`	aws:ResourceTag/${TagKey}
autoscalingconfiguration	`arn:${Partition}:apprunner:${Region}:${Account}:autoscalingconfiguration/${AutoscalingConfigurationName}/${AutoscalingConfigurationVersion}/${AutoscalingConfigurationId}`	aws:ResourceTag/${TagKey}
observabilityconfiguration	`arn:${Partition}:apprunner:${Region}:${Account}:observabilityconfiguration/${ObservabilityConfigurationName}/${ObservabilityConfigurationVersion}/${ObservabilityConfigurationId}`	aws:ResourceTag/${TagKey}
vpcconnector	`arn:${Partition}:apprunner:${Region}:${Account}:vpcconnector/${VpcConnectorName}/${VpcConnectorVersion}/${VpcConnectorId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
vpcingressconnection	arn:${Partition}:apprunner:${Region}:${Account}:vpcingressconnection/${VpcIngressConnectionName}/${VpcIngressConnectionId}	aws:ResourceTag/${TagKey}
webacl	arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/webacl/${Name}/${Id}	

Bedingungsschlüssel für AWS App Runner

AWS App Runner definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
apprunner:AutoScalingConfigurationArn	Filtert den Zugriff auf die Aktionen CreateService und UpdateService basierend auf dem ARN einer zugehörigen AutoScalingConfiguration-Ressource	ARN
apprunner:ConnectionArn	Filtert den Zugriff auf die Aktionen CreateService und UpdateService basierend auf dem ARN einer zugehörigen Verbindungsressource	ARN
apprunner:Observab	Filtert den Zugriff auf die Aktionen CreateService und UpdateService basierend auf dem ARN einer zugehörig	ARN

Bedingungsschlüssel	Beschreibung	Typ
ilityConfigurationArn	en Beobachtbarkeits-Konfigurationsressource (ObservabilityConfiguration)	
apprunner:ServiceArn	Filtert den Zugriff auf die Aktion CreateVpcIngressConnection basierend auf dem ARN einer zugehörigen Service-Ressource	ARN
apprunner:VpcConnectorArn	Filtert den Zugriff auf die Aktionen CreateService und UpdateService basierend auf dem ARN einer zugehörigen VPC-Verbindungsressource	ARN
apprunner:VpcEndpointId	Filtert den Zugriff auf die Aktionen CreateVpcIngressConnection und UpdateVpcIngressConnection basierend auf dem VPC-Endpunkt in der Anfrage	Zeichenfolge
apprunner:VpcId	Filtert den Zugriff auf die Aktionen CreateVpcIngressConnection und UpdateVpcIngressConnection basierend auf dem VPC in der Anfrage	Zeichenfolge
aws:RequestTag/${TagKey}	Filtert den Zugriff danach, ob Tag-Schlüssel-Wert-Paare in der Anforderung vorhanden sind	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tag-Schlüssel-Wert-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert Zugriff basierend auf dem Vorhandensein von Tag-Schlüsseln in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS-App2Container

AWS-App2Container (Service-Präfix: `a2c`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS-App2Container definierte Aktionen
- Von AWS-App2Container definierte Ressourcentypen
- Bedingungsschlüssel für AWS-App2Container

Von AWS-App2Container definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetContainerizationJobDetails	Gewährt die Berechtigung zum Abrufen der Details aller Containerisierungsaufträge	Lesen			
GetDeploymentJobDetails	Gewährt die Berechtigung zum Abrufen der Details aller Bereitstellungsaufträge	Lesen			
StartContainerizationJob	Gewährt die Berechtigung zum Starten eines Containerisierungsauftrags	Schreiben			
StartDeploymentJob	Gewährt die Berechtigung zum Starten eines Bereitstellungsauftrags	Schreiben			

Von AWS-App2Container definierte Ressourcentypen

AWS-App2Container unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf AWS-App2Container zuzulassen, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS-App2Container

App2Container verfügt über keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS AppConfig

AWS AppConfig (Servicepräfix: `appconfig`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS AppConfig definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich

sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateApplication	Gewährt die Berechtigung zum Erstellen einer Anwendung	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfigurationProfile	Gewährt die Berechtigung zum Erstellen eines Konfigurationsprofils	Write	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeploymentStrategy	Gewährt die Berechtigung zum Erstellen einer Bereitstellungsstrategie	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironment	Gewährt die Berechtigung zum Erstellen einer Umgebung	Schreiben	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExtension	Erteilung der Berechtigung zur Erstellung einer Erweiterung	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateExtensionAssociation	Erteilung der Berechtigung zur Erstellung einer Erweiterungsassoziation	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateHostedConfigurationVersion	Gewährt die Berechtigung zum Erstellen einer gehosteten Konfigurationsversion	Write	application*		
			configurationprofile*		
DeleteApplication	Gewährt die Berechtigung zum Löschen einer Anwendung	Write	application*		
DeleteConfigurationProfile	Gewährt die Berechtigung zum Löschen eines Konfigurationsprofils	Write	application*		
			configurationprofile*		
DeleteDeploymentStrategy	Gewährt die Berechtigung zum Löschen einer Bereitstellungsstrategie	Write	deploymentstrategy*		
DeleteEnvironment	Gewährt die Berechtigung zum Löschen einer Umgebung	Schreiben	application*		
			environment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteExtension	Erteilung der Berechtigung zum Löschen einer Erweiterung	Schreiben	extension*		
DeleteExtensionAssociation	Erteilung der Berechtigung zum Löschen einer Erweiterungs-Zuordnung	Schreiben	extensionassociation*		
DeleteHostedConfigurationVersion	Gewährt die Berechtigung zum Löschen einer gehosteten Konfigurationsversion	Write	application*		
			configurationprofile*		
			hostedconfigurationversion*		
GetApplication	Gewährt die Berechtigung zum Anzeigen von Details zu einer Anwendung	Read	application*		
				aws:ResourceTag/${TagKey}	
GetConfiguration	Gewährt die Berechtigung zum Anzeigen von Details zu einer Konfiguration	Read	application*		
			configurationprofile*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			environment*		
				aws:ResourceTag/${TagKey}	
GetConfigurationProfile	Gewährt die Berechtigung zum Anzeigen von Details zu einem Konfigurationsprofil	Read	application*		
			configurationprofile*		
				aws:ResourceTag/${TagKey}	
GetDeployment	Gewährt die Berechtigung zum Anzeigen von Details zu einer Bereitstellung	Read	application*		
			deployment*		
			environment*		
				aws:ResourceTag/${TagKey}	
GetDeploymentStrategy	Gewährt die Berechtigung zum Anzeigen von Details zu einer Bereitstellungsstrategie	Read	deploymentstrategy*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
GetEnvironment	Gewährt die Berechtigung zum Anzeigen von Details zu einer Umgebung	Lesen	application*		
			environment*		
				aws:ResourceTag/${TagKey}	
GetExtension	Erteilung der Berechtigung zur Anzeige von Details zu einer Erweiterung	Lesen	extension*		
				aws:ResourceTag/${TagKey}	
GetExtensionAssociation	Erteilung der Berechtigung zur Anzeige von Details über eine Erweiterungs-Zuordnung	Lesen	extensionassociation*		
				aws:ResourceTag/${TagKey}	
GetHostedConfigurationVersion	Gewährt die Berechtigung zum Anzeigen von Details zu einer gehosteten Konfigurationsversion	Lesen	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			configurationprofile*		
			hostedconfigurationversion*		
GetLatestConfiguration	Gewährt die Berechtigung zum Abrufen einer bereitgestellten Konfiguration	Lesen	configuration*		
				aws:ResourceTag/${TagKey}	
ListApplications	Gewährt die Berechtigung zum Auflisten der Anwendungen in Ihrem Konto	List			
ListConfigurationProfiles	Gewährt die Berechtigung zum Auflisten der Konfigurationsprofile für eine Anwendung	List	application*		
ListDeploymentStrategies	Gewährt die Berechtigung zum Auflisten der Bereitstellungsstrategien für Ihr Konto	List			
ListDeployments	Gewährt die Berechtigung zum Auflisten der Bereitstellungen für eine Umgebung	List	application*		
			environment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListEnvironments	Gewährt die Berechtigung zum Auflisten der Umgebungen für eine Anwendung	Auflisten	application*		
ListExtensionAssociations	Erteilung der Berechtigung zur Auflistung der Erweiterungs-Zuordnungen in Ihrem Konto	Auflisten			
ListExtensions	Erteilung der Berechtigung zur Auflistung der Erweiterungen in Ihrem Konto	Auflisten			
ListHostedConfigurationVersions	Gewährt die Berechtigung zum Auflisten der gehosteten Konfigurationsversionen für ein Konfigurationsprofil	List	application*		
			configurationprofile*		
ListTagsForResource	Gewährt die Berechtigung zum Anzeigen einer Liste von Ressourcen-Tags für eine angegebene Ressource.	Lesen	application		
			configurationprofile		
			deployment		
			deploymentstrategy		
			environment		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			extension		
			extension association		
				aws:ResourceTag/${TagKey}	
StartConfiguration Session	Gewährt die Berechtigung zum Starten einer Konfigurationssitzung	Schreiben	configuration*		
				aws:ResourceTag/${TagKey}	
StartDeployment	Gewährt die Berechtigung zum Initiieren einer Bereitstellung	Write	application*		
			configurationprofile*		
			deploymentstrategy*		
			environment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
StopDeployment	Gewährt die Berechtigung zum Beenden einer Bereitstellung	Schreiben	application*		
			deployment*		
			environment*		
TagResource	Gewährt die Berechtigung zum Versehen einer appconfig-Ressource mit einem Tag	Markierung	application		
			configuration		
			configurationprofile		
			deployment		
			deploymentstrategy		
			environment		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			extension		
			extension association		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer appconfig-Ressource	Markierung	application		
			configuration		
			configurationprofile		
			deployment		
			deploymentstrategy		
			environment		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			extension		
			extension association		
				aws:TagKeys	
UpdateApplication	Gewährt die Berechtigung zum Ändern einer Anwendung	Write	application*		
				aws:ResourceTag/${TagKey}	
UpdateConfigurationProfile	Gewährt die Berechtigung zum Ändern eines Konfigurationsprofils	Write	application*		
			configurationprofile*		
				aws:ResourceTag/${TagKey}	
UpdateDeploymentStrategy	Gewährt die Berechtigung zum Ändern einer Bereitstellungsstrategie	Write	deploymentstrategy*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateEnvironment	Gewährt die Berechtigung zum Ändern einer Umgebung	Schreiben	application*		
			environment*		
				aws:ResourceTag/${TagKey}	
UpdateExtension	Erteilung der Berechtigung zur Änderung einer Erweiterung	Schreiben	extension*		
				aws:ResourceTag/${TagKey}	
UpdateExtensionAssociation	Erteilung der Berechtigung zur Änderung einer Erweiterungs-Zuordnung	Schreiben	extensionassociation*		
				aws:ResourceTag/${TagKey}	
ValidateConfiguration	Gewährt die Berechtigung zum Validieren einer Konfiguration	Write	application*		
			configurationprofile*		

Von AWS AppConfig definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
application	`arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}`	aws:ResourceTag/${TagKey}
environment	`arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/environment/${EnvironmentId}`	aws:ResourceTag/${TagKey}
configurationprofile	`arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/configurationprofile/${ConfigurationProfileId}`	aws:ResourceTag/${TagKey}
deploymentstrategy	`arn:${Partition}:appconfig:${Region}:${Account}:deploymentstrategy/${DeploymentStrategyId}`	aws:ResourceTag/${TagKey}
deployment	`arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/environment/${EnvironmentId}/deployment/${DeploymentNumber}`	aws:ResourceTag/${TagKey}
hostedconfigurationversion	`arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/configurationprofile/${Configur`	

Ressourcentypen	ARN	Bedingungsschlüssel
	`ationProfileId}/hostedconfigurationversion/${VersionNumber}`	
configuration	`arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/environment/${EnvironmentId}/configuration/${ConfigurationProfileId}`	aws:ResourceTag/${TagKey}
extension	`arn:${Partition}:appconfig:${Region}:${Account}:extension/${ExtensionId}/${ExtensionVersionNumber}`	aws:ResourceTag/${TagKey}
extension association	`arn:${Partition}:appconfig:${Region}:${Account}:extensionassociation/${ExtensionAssociationId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS AppConfig

AWS AppConfig definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem erlaubten Satz von Werten für einen angegebenen Tag	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach einem der AWS-Ressource zugewiesenen Tag-Schlüssel-Wert-Paar	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach Liste von Tag-Schlüsseln, die in der Anforderung zulässig sind	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS AppFabric

AWS AppFabric (Servicepräfix: `appfabric`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS AppFabric definierte Aktionen
- Von AWS AppFabric definierte Ressourcentypen
- Bedingungsschlüssel für AWS AppFabric

Von AWS AppFabric definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetUserAccessTasks	Gewährt die Berechtigung, Benutzerzugriffsaufgaben für mehrere Benutzer zu starten	Schreiben	appbundle*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ConnectAppAuthorization	Gewährt die Berechtigung zum Verbinden von Anwendungsautorisierungen	Schreiben	appauthorization*		
CreateAppAuthorization	Gewährt die Berechtigung zum Erstellen von Anwendungsautorisierungen für Anwendungspakete	Schreiben	appbundle*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAppBundle	Gewährt die Berechtigung zum Erstellen von Anwendungspaketen in Ihrem Konto	Schreiben	appbundle*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIngestion	Gewährt die Berechtigung zum Erstellen von Aufnahmen für Anwendungspakete	Schreiben	appbundle*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateIngestionDestination	Gewährt die Berechtigung zum Erstellen von Aufnahmezielen für Anwendungspakete	Schreiben	appbundle*		
			ingestion*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAppAuthorization	Gewährt die Berechtigung zum Löschen von Anwendungsautorisierungen in einem Anwendungspaket	Schreiben	appauthorization*		
DeleteAppBundle	Gewährt die Berechtigung zum Löschen von Anwendungspaketen in Ihrem Konto	Schreiben	appbundle*		
DeleteIngestion	Gewährt die Berechtigung zum Löschen von Aufnahmen in einem Anwendungspaket	Schreiben	ingestion*		
DeleteIngestionDestination	Gewährt die Berechtigung, Ziele in einer Aufnahme zu löschen	Schreiben	ingestiondestination*		
GetAppAuthorization	Gewährt die Berechtigung zum Anzeigen von Details zu Anwendungsautorisierungen	Lesen	appauthorization*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			appbundle*		
				aws:ResourceTag/${TagKey}	
GetAppBundle	Gewährt die Berechtigung zum Anzeigen von Details zu Anwendungspaketen	Lesen	appbundle*		
				aws:ResourceTag/${TagKey}	
GetIngestion	Gewährt die Berechtigung, Details zu Aufnahmen anzuzeigen	Lesen	appbundle*		
			ingestion*		
				aws:ResourceTag/${TagKey}	
GetIngestionDestination	Gewährt die Berechtigung, Details zu Aufnahmezielen anzuzeigen	Lesen	appbundle*		
			ingestion*		
			ingestiondestination*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
ListAppAuthorizations	Gewährt die Berechtigung zum Abrufen einer Liste der Anwendungsautorisierungen in einem Anwendungspaket	Auflisten	appbundle*		
ListAppBundles	Gewährt die Berechtigung zum Abrufen einer Liste der Anwendungspakete in Ihrem Konto	Auflisten			
ListIngestionDestinations	Gewährt die Berechtigung, eine Liste der Ziele in einer Aufnahme abzurufen	Auflisten	appbundle*		
			ingestion*		
ListIngestions	Gewährt die Berechtigung zum Abrufen einer Liste der Aufnahmen in einem Anwendungspaket	Auflisten	appbundle*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für AppFabric-Ressourcen	Lesen	appauthorization		
			appbundle		
			ingestion		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			ingestiondestination		
StartIngestion	Gewährt die Berechtigung, Aufnahmen zu starten	Schreiben	ingestion*		
StartUserAccessTasks	Gewährt die Berechtigung, Benutzerzugriffsaufgaben zu starten	Schreiben	appbundle*		
StopIngestion	Gewährt die Berechtigung, Aufnahmen zu stoppen	Schreiben	ingestion*		
TagResource	Gewährt die Berechtigung, AppFabric-Ressourcen zu taggen	Markierung	appauthorization		
			appbundle		
			ingestion		
			ingestiondestination		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Gewährt die Berechtigung, Tags von AppFabric-Ressourcen zu entfernen	Markierung	appauthorization		
			appbundle		
			ingestion		
			ingestiondestination		
				aws:TagKeys	
UpdateAppAuthorization	Gewährt die Berechtigung zum Aktualisieren von Anwendungsautorisierungen in Anwendungspaketen	Schreiben	appauthorization*		
			appbundle*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateIngestionDestination	Gewährt die Berechtigung, Ziele in Aufnahmen zu aktualisieren	Schreiben	appbundle*		
			ingestion*		
			ingestiondestination*		
				aws:ResourceTag/${TagKey}	

Von AWS AppFabric definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
appbundle	`arn:${Partition}:appfabric:${Region}:${Account}:appbundle/${AppBundleIdentifier}`	aws:ResourceTag/${TagKey}
appauthorization	`arn:${Partition}:appfabric:${Region}:${Account}:appbundle/${AppbundleId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
	`/appauthorization/${AppAuthorizationIdentifier}`	
ingestion	`arn:${Partition}:appfabric:${Region}:${Account}:appbundle/${AppbundleId}/ingestion/${IngestionIdentifier}`	aws:ResourceTag/${TagKey}
ingestion destination	`arn:${Partition}:appfabric:${Region}:${Account}:appbundle/${AppbundleId}/ingestion/${IngestionIdentifier}/ingestiondestination/${IngestionDestinationIdentifier}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS AppFabric

AWS AppFabric definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon AppFlow

Amazon AppFlow (Servicepräfix: `appflow`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon AppFlow definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelFlowExecutions	Gewährt die Berechtigung zum Abbrechen der laufenden Ausführungen eines Amazon AppFlow-Flows	Schreiben	flow*		
CreateConnectorProfile	Gewährt die Berechtigung zum Erstellen eines Anmeldeprofils, das mit Amazon AppFlow-Flows verwendet werden soll	Write			
CreateFlow	Gewährt die Berechtigung zum Erstellen eines Amazon AppFlow-Flow	Write		aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
DeleteConnectorProfile	Gewährt die Berechtigung zum Löschen eines in Amazon AppFlow konfigurierten Anmeldeprofils	Write	connectorprofile*		
DeleteFlow	Gewährt die Berechtigung zum Löschen eines Amazon AppFlow-Flow	Schreiben	flow*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeConnector	Gewährt die Berechtigung zum Beschreiben eines Konnektors, der im Amazon AppFlow registriert ist	Lesen	connector*		
DescribeConnectorEntity	Gewährt die Berechtigung, alle Felder für ein Objekt in einem in Amazon AppFlow konfigurierten Anmeldeprofil zu beschreiben	Read	connectorprofile*		
DescribeConnectorFields [nur Berechtigung]	Gewährt die Berechtigung, alle Felder für ein Objekt in einem in Amazon AppFlow konfigurierten Anmeldeprofil zu beschreiben (nur Konsole)	Read	connectorprofile*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeConnectorProfiles	Gewährt die Berechtigung zum Beschreiben aller in Amazon AppFlow konfigurierten Anmeldeprofile	Read			
DescribeConnectors	Gewährt die Berechtigung zum Beschreiben aller Connectors, die von Amazon AppFlow unterstützt werden	Read			
DescribeFlow	Gewährt die Berechtigung zum Beschreiben eines bestimmten in Amazon AppFlow konfigurierten Abläufen	Read	flow*		
DescribeFlowExecution [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben aller Ablauf-Ausführungen für einen in Amazon AppFlow konfigurierten Ablauf (nur Konsole)	Read	flow*		
DescribeFlowExecutionRecords	Gewährt die Berechtigung zum Beschreiben aller Ablauf-Ausführungen für einen in Amazon AppFlow konfigurierten Ablauf	Read	flow*		
DescribeFlows [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben aller in Amazon AppFlow konfigurierten Abläufe (nur Konsole)	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListConnectorEntities	Gewährt die Berechtigung, alle Objekte für ein in Amazon AppFlow konfiguriertes Anmeldeprofil aufzulisten	List	connectorprofile*		
ListConnectorFields [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aller Objekte für ein in Amazon AppFlow konfiguriertes Anmeldeprofil (nur Konsole)	Lesen	connectorprofile*		
ListConnectors	Gewährt die Berechtigung zum Beschreiben aller Konnektoren, die von Amazon AppFlow unterstützt werden	Auflisten	connector*		
ListFlows	Gewährt die Berechtigung zum Auflisten aller in Amazon AppFlow konfigurierten Abläufe	List	flow*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für einen Ablauf	Lesen	flow*		
RegisterConnector	Gewährt die Berechtigung zum Registrieren eines Amazon-AppFlow-Konnektors	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ResetConnectorMetadataCache	Gewährt die Berechtigung, Metadaten von Connector-Entitäten zurückzusetzen, die Amazon AppFlow im Cache gespeichert hat	Schreiben	connectorprofile*		
RunFlow [nur Berechtigung]	Gewährt die Berechtigung zum Ausführen eines in Amazon AppFlow konfigurierten Ablaufs (nur Konsole)	Write	flow*		
StartFlow	Gewährt die Berechtigung zum Aktivieren (für geplante und ereignisgesteuerte Abläufe) oder Ausführen (für bedarfsgesteuerte Abläufe) eines in Amazon AppFlow konfigurierten Ablaufs	Write	flow*		
StopFlow	Gewährt die Berechtigung zum Deaktivieren eines geplanten oder ereignisgesteuerten Ablaufs, der in Amazon AppFlow konfiguriert ist	Schreiben	flow*		
TagResource	Gewährt die Berechtigung, einen Ablauf oder einen Connector zu taggen	Markierung	connector		
			flow		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
UnRegisterConnector	Gewährt die Berechtigung zur Aufhebung der Registrierung eines Amazon-AppFlow-Konnektors	Schreiben	connector*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung, Tags von einem Ablauf oder einem Connector zu entfernen	Markierung	connector		
			flow		
				aws:TagKeys	
UpdateConnectorProfile	Gewährt die Berechtigung zum Aktualisieren eines in Amazon AppFlow konfigurierten Anmeldeprofils	Schreiben	connectorprofile*		
UpdateConnectorRegistration	Gewährt die Berechtigung zum Aktualisieren eines in Amazon AppFlow konfigurierten registrierten Konnektors	Schreiben	connector*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateFlow	Gewährt die Berechtigung zum Aktualisieren eines in Amazon AppFlow konfigurierten Ablaufs	Write	flow*		
UseConnectorProfile [nur Berechtigung]	Gewährt die Berechtigung zur Verwendung eines Konnektorprofils beim Erstellen eines Ablaufs in Amazon AppFlow	Write	connectorprofile*		

Von Amazon AppFlow definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
connectorprofile	`arn:${Partition}:appflow:${Region}:${Account}:connectorprofile/${ProfileName}`	
flow	`arn:${Partition}:appflow:${Region}:${Account}:flow/${FlowName}`	aws:ResourceTag/${TagKey}
connector	`arn:${Partition}:appflow:${Region}:${Account}:connector/${ConnectorLabel}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon AppFlow

Amazon AppFlow definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den zulässigen Werten für jedes der Tags	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Tag-Wert, der der Ressource zugeordnet ist	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach dem Vorhandensein verbindlicher Tags in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon AppIntegrations

Amazon AppIntegrations (Servicepräfix: `app-integrations`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon AppIntegrations definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateApplication	Gewährt die Berechtigung zum Erstellen einer neuen Anwendung	Schreiben	application*		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateApplicationAssociation [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer Anwendungszuweisung	Schreiben	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDataIntegration	Gewährt Berechtigungen zum Erstellen einer neuen DataIntegration	Schreiben	data-integration*		appflow:DeleteFlow appflow:DescribeConnectorProfiles iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy kms:CreateGrant s3:GetBucketNotification s3:GetEncryptionConfiguration s3:PutBucketNotification

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataIntegrationAssociation [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer DataIntegrationAssociation	Schreiben	data-integration*		appflow:CreateFlow appflow:DeleteFlow appflow:DescribeConnectorEntity appflow:DescribeConnectorProfiles appflow:TagResource appflow:UseConnectorProfile

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventIntegration	Gewährt die Berechtigung zum Erstellen einer neuen EventIntegration	Schreiben	event-integration*		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventIntegrationAssociation [nur Berechtigung]	Gewährt die Berechtigungen zum Erstellen einer EventIntegrationAssociation	Schreiben	event-integration*		events:PutRule events:PutTargets

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Gewährt die Berechtigung zum Löschen einer Anwendung	Schreiben	application*		
				aws:ResourceTag/${TagKey}	
DeleteApplicationAssociation [nur Berechtigung]	Gewährt die Berechtigung zum Löschen einer Anwendungszuweisung	Schreiben	application-association*		
DeleteDataIntegration	Gewährt die Berechtigung zum Löschen einer DataIntegration	Schreiben	data-integration*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteDataIntegrationAssociation [nur Berechtigung]	Gewährt die Berechtigung zum Löschen einer DataIntegrationAssociation	Schreiben	data-integration-association*		appflow:CreateFlow appflow:DeleteFlow appflow:DescribeConnectorEntity appflow:DescribeConnectorProfiles appflow:StopFlow appflow:TagResource appflow:UseConnectorProfile
DeleteEventIntegration	Gewährt die Berechtigung zum Löschen einer EventIntegration	Schreiben	event-integration*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteEventIntegrationAssociation [nur Berechtigung]	Gewährt die Berechtigung zum Löschen einer EventIntegrationAssociation	Schreiben	event-integration-association*		events:DeleteRule events:ListTargetsByRule events:RemoveTargets
GetApplication	Gewährt die Berechtigung zum Anzeigen von Details zu einer Anwendung	Lesen	application*		
				aws:ResourceTag/${TagKey}	
GetDataIntegration	Gewährt die Berechtigung zum Anzeigen von Details zu DataIntegrations	Read	data-integration*		
				aws:ResourceTag/${TagKey}	
GetEventIntegration	Gewährt die Berechtigung zum Anzeigen von Details zu EventIntegrations	Lesen	event-integration*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListApplicationAssociations	Gewährt die Berechtigung zum Auflisten von Anwendungszuordnungen	Auflisten			
ListApplications	Gewährt die Berechtigung zum Auflisten von Anwendungen	Auflisten			
ListDataIntegrationAssociations	Gewährt die Berechtigung zum Auflisten von DataIntegrationAssociations	Auflisten			
ListDataIntegrations	Gewährt die Berechtigung zum Auflisten von DataIntegrations	Auflisten			
ListEventIntegrationAssociations	Gewährt die Berechtigung zum Auflisten von EventIntegrationAssociations	Lesen			
ListEventIntegrations	Gewährt die Berechtigung zum Auflisten von EventIntegrations	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Amazon AppIntegration-Resource	Read	application		
			data-integration		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			data-integration-association		
			event-integration		
			event-integration-association		
				aws:ResourceTag/${TagKey}	
TagResource	Gewährt die Berechtigung zum Markieren einer Amazon AppIntegration-Ressource	Tagging	application		
			application-association		
			data-integration		
			data-integration-association		
			event-integration		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			event-integration-association		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Amazon-AppIntegration-Ressource.	Tagging	application		
			application-association		
			data-integration		
			data-integration-association		
			event-integration		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			event-integration-association		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateApplication	Gewährt die Berechtigung zum Ändern einer Anwendung	Schreiben	application*		
				aws:ResourceTag/${TagKey}	
UpdateDataIntegration	Gewährt die Berechtigung zum Ändern einer DataIntegration	Schreiben	data-integration*		
				aws:ResourceTag/${TagKey}	
UpdateEventIntegration	Gewährt die Berechtigung zum Ändern einer EventIntegration	Schreiben	event-integration*		
				aws:ResourceTag/${TagKey}	

Von Amazon AppIntegrations definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
event-integration	`arn:${Partition}:app-integrations:${Region}:${Account}:event-integration/${EventIntegrationName}`	aws:ResourceTag/${TagKey}
event-integration-association	`arn:${Partition}:app-integrations:${Region}:${Account}:event-integration-association/${EventIntegrationName}/${ResourceId}`	aws:ResourceTag/${TagKey}
data-integration	`arn:${Partition}:app-integrations:${Region}:${Account}:data-integration/${DataIntegrationId}`	aws:ResourceTag/${TagKey}
data-integration-association	`arn:${Partition}:app-integrations:${Region}:${Account}:data-integration-association/${DataIntegrationId}/${ResourceId}`	aws:ResourceTag/${TagKey}
application	`arn:${Partition}:app-integrations:${Region}:${Account}:application/${ApplicationId}`	aws:ResourceTag/${TagKey}
application-association	`arn:${Partition}:app-integrations:${Region}:${Account}:application-association/${ApplicationId}/${ApplicationAssociationId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon AppIntegrations

Amazon AppIntegrations definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch Tags, die in der Anforderung übergeben werden	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf Tags, die der Ressource zugeordnet sind	String
aws:TagKeys	Filtert den Zugriff basierend auf Tag-Schlüsseln, die in der Anforderung übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Application Auto Scaling

AWS Application Auto Scaling (Servicepräfix: `application-autoscaling`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Application Auto Scaling definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteScalingPolicy	Gewährt die Berechtigung zum Löschen einer Skalierungsrichtlinie	Schreiben	ScalableTarget*		
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
DeleteScheduledAction	Gewährt die Berechtigung zum Löschen einer geplanten Aktion	Schreiben	ScalableTarget*		
				application-autoscaling:service-	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				namespace application-autoscaling:scalable-dimension	
DeregisterScalableTarget	Gewährt die Berechtigung zum Aufheben der Registrierung eines skalierbaren Ziels	Schreiben	ScalableTarget*		
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
DescribeScalableTargets	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer skalierbarer Ziele im angegebenen Namespace	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeScalingActivities	Gewährt die Berechtigung, eine Reihe von Skalierungsaktivitäten oder alle Skalierungsaktivitäten im angegebenen Namespace zu beschreiben	Lesen			
DescribeScalingPolicies	Gewährt die Berechtigung, eine Reihe von Skalierungsrichtlinien oder alle Skalierungsrichtlinien im angegebenen Namespace zu beschreiben	Lesen			
DescribeScheduledActions	Gewährt die Berechtigung, eine Reihe geplanter Aktionen oder alle geplanten Aktionen im angegebenen Namespace zu beschreiben	Lesen			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für ein skalierbares Ziel	Lesen	ScalableTarget*		
PutScalingPolicy	Gewährt die Berechtigung zum Erstellen und Aktualisieren einer Skalierungsrichtlinie für ein skalierbares Ziel	Schreiben	ScalableTarget*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
PutScheduledAction	Gewährt die Berechtigung zum Erstellen und Aktualisieren einer geplanten Aktion für ein skalierbares Ziel	Schreiben	ScalableTarget*		
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RegisterScalableTarget	Erteilt die Berechtigung zum Registrieren von AWS oder von benutzerdefinierten Ressourcen als skalierbare Ziele mit Application Auto Scaling und zur Aktualisierung von Konfigurationsparametern zur Verwaltung eines skalierbaren Ziels	Schreiben	ScalableTarget*		application-autoscaling:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
TagResource	Gewährt die Berechtigung zum Markieren eines skalierbaren Ziels	Markierung	ScalableTarget*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags von einem skalierbaren Ziel	Markierung	ScalableTarget*		
				aws:TagKeys	

Von AWS Application Auto Scaling definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
ScalableTarget	`arn:${Partition}:application-autoscaling:${Region}:${Account}:scalable-target/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Application Auto Scaling

AWS Application Auto Scaling definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
application-autoscaling:scalable-dimension	Filtert den Zugriff durch die skalierbare Dimension, die in der Anforderung übergeben wird	Zeichenfolge
application-autoscaling:service-namespace	Filtert den Zugriff nach dem Service-Namespace, der in der Anforderung übergeben wird	Zeichenfolge
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS-Application-Cost-Profiler-Service

AWS-Application-Cost-Profiler-Service (Servicepräfix: `application-cost-profiler`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Vom AWS-Application-Cost-Profiler-Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteReportDefinition	Gewährt die Berechtigung zum Löschen der Konfiguration mit einem angegebenen Application-Cost-Profiler-Bericht, wodurch die Berichtsgenerierung effektiv deaktiviert wird	Write			
GetReportDefinition	Gewährt die Berechtigung zum Abrufen der Konfiguration mit einer angegebenen Application-Cost-Profiler-Berichtsanforderung	Read			
ImportApplicationUsage	Gewährt die Berechtigung zum Importieren der Anwendungsnutzung aus S3	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListReportDefinitions	Gewährt die Berechtigung zum Abrufen einer Liste der verschiedenen von ihnen erstellten Konfigurationen des Application-Cost-Profiler-Berichts	Read			
PutReportDefinition	Gewährt die Berechtigung zum Erstellen von Konfigurationen für den Application-Cost-Profiler-Bericht	Write			
UpdateReportDefinition	Gewährt die Berechtigung zum Aktualisieren einer vorhandenen Konfiguration des Application-Cost Profiler-Berichts	Write			

Vom AWS-Application-Cost-Profiler-Service definierte Ressourcentypen

AWS-Application-Cost-Profiler-Service unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf AWS-Application-Cost-Profiler-Service zu ermöglichen, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS-Application-Cost-Profiler-Service

Application Cost Profiler besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` der Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Application Discovery Arsenal

Application Discovery (Servicepräfix: `arsenal`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Application Discovery Arsenal definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RegisterOnPremisesAgent [nur Berechtigung]	Gewährt die Berechtigung zur Registrierung der von AWS bereitgestellten Datensammler für Application Discovery Service	Write			

Von Application Discovery Arsenal definierte Ressourcentypen

Application Discovery Arsenal unterstützt nicht die Angabe eines Ressourcen-ARNs im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf Application Discovery Arsenal zu ermöglichen, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für Application Discovery Arsenal

Application Discovery besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Application Discovery Service

AWS Der Application Discovery Service (Dienstpräfix:`discovery`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Application Discovery Service definierte Aktionen
- Von AWS Application Discovery Service definierte Ressourcentypen
- Bedingungsschlüssel für AWS Application Discovery Service

Von AWS Application Discovery Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn

die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateConfigurationItemsToApplication	Erteilt der API die Berechtigung. AssociateConfigurationItemsToApplication AssociateConfigurationItemsToApplication ordnet einer Anwendung ein oder mehrere Konfigurationselemente zu	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchDeleteAgents	Erteilt der BatchDeleteAgents API die Erlaubnis. BatchDeleteAgents löscht einen oder mehrere mit Ihrem Konto verknüpfte Agenten/Datensammelpunkte, die jeweils anhand ihrer Agenten-ID identifiziert werden. Durch das Löschen eines Datensammelpunkts werden die zuvor erfassten Daten nicht gelöscht	Schreiben			
BatchDeleteImportData	Erteilt der API die Erlaubnis . BatchDeleteImportData BatchDeleteImportData löscht eine oder mehrere Migration Hub Hub-Importaufgaben, die jeweils durch ihre Import-ID identifiziert werden. Jede Importaufgabe verfügt über eine Reihe von Datensätzen, die Server oder Anwendungen identifizieren können	Schreiben			
CreateApplication	Erteilt der CreateApplication API die Erlaubnis . CreateApplication erstellt eine Anwendung mit dem angegebenen Namen und der Beschreibung	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTags	Erteilt der CreateTags API die Erlaubnis. CreateTags erstellt ein oder mehrere Tags für Konfigurationselemente. Tags sind Metadaten zur Kategorisierung von IT-Komponenten. Diese API akzeptiert eine Liste mit mehreren Konfigurationselementen	Tagging			
DeleteApplications	Erteilt der DeleteApplications API die Erlaubnis. DeleteApplications löscht eine Liste von Anwendungen und deren Verknüpfungen zu Konfigurationselementen	Schreiben			
DeleteTags	Erteilt der DeleteTags API die Erlaubnis. DeleteTags löscht die Zuordnung zwischen Konfigurationselementen und einem oder mehreren Tags. Diese API akzeptiert eine Liste mit mehreren Konfigurationselementen	Tagging		aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeAgents	Erteilt der DescribeAgents API die Erlaubnis. DescribeAgents listet Agenten oder den Connector nach ID auf oder listet alle Agenten/Connectors auf, die Ihrem Benutzer zugeordnet sind, sofern Sie keine ID angegeben haben	Lesen			
DescribeBatchDeleteConfigurationTask	Erteilt der API die Erlaubnis. DescribeBatchDeleteConfigurationTask DescribeBatchDeleteConfigurationTask gibt Attribute zu einer Batch-Löschaufgabe zurück, mit der eine Reihe von Konfigurationselementen gelöscht werden sollen. Die angegebene Aufgaben-ID sollte die Aufgaben-ID sein, die aus der Ausgabe von abgerufen wurde StartBatchDeleteConfigurationTask	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeConfigurations	Erteilt der DescribeConfigurations API die Erlaubnis. DescribeConfigurations ruft Attribute für eine Liste von Konfigurationselement-IDs ab. Alle bereitgestellten IDs müssen sich auf denselben Komponententyp (Server, Anwendung, Prozess oder Verbindung) beziehen. Ausgabefelder sind für den gewählten Komponententyp spezifisch. Beispiel: Die Ausgabe für ein Server-Konfigurationselement enthält eine Liste von Attributen zum Server, z. B. den Host-Namen, das Betriebssystem und die Anzahl der Netzwerkkarten	Lesen			
DescribeContinuousExports	Erteilt der DescribeContinuousExports API die Erlaubnis. DescribeContinuousExports listet Exporte gemäß der ID auf. Alle kontinuierlichen Exporte, die Ihrem Benutzer zugeordnet sind, können aufgelistet werden, wenn Sie sie DescribeContinuousExports unverändert aufrufen, ohne Parameter zu übergeben	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeExportConfigurations	Erteilt der DescribeExportConfigurations API die Erlaubnis. DescribeExportConfigurations ruft den Status eines bestimmten Exportvorgangs ab. Sie können den Status von maximal 100 Prozessen abrufen	Lesen			
DescribeExportTasks	Erteilt der DescribeExportTasks API die Erlaubnis. DescribeExportTasks ruft den Status einer oder mehrerer Exportaufgaben ab. Sie können den Status von bis zu 100 Exportaufgaben abrufen	Lesen			
DescribeImportTasks	Erteilt der DescribeImportTasks API die Erlaubnis. DescribeImportTasks gibt eine Reihe von Importaufgaben für Ihren Benutzer zurück, darunter Statusinformationen, Zeiten, IDs, die Amazon S3 S3-Objekt-URL für die Importdatei und mehr	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeTags	Erteilt der DescribeTags API die Erlaubnis. DescribeTags ruft eine Liste von Konfigurationselementen ab, die mit einem bestimmten Tag gekennzeichnet sind. Ruft alternativ eine Liste aller Tags ab, die einem bestimmten Konfigurationselement zugewiesen sind	Lesen			
DisassociateConfigurationItemsFromApplication	Erteilt der DisassociateConfigurationItemsFromApplication API die Erlaubnis. DisassociateConfigurationItemsFromApplication trennt ein oder mehrere Konfigurationselemente von einer Anwendung	Schreiben			
ExportConfigurations	Erteilt der ExportConfigurations API die Erlaubnis. ExportConfigurations exportiert alle erkannten Konfigurationsdaten in einen Amazon S3 S3-Bucket oder eine Anwendung, mit der Sie die Daten anzeigen und auswerten können. Zu den Daten gehören Tags und Tag-Zuordnungen, Prozesse, Verbindungen, Server und Systemleistung	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDiscoverySummary	Erteilt der GetDiscoverySummary API die Erlaubnis. GetDiscoverySummary ruft eine kurze Zusammenfassung der entdeckten Ressourcen ab	Lesen			
GetNetworkConnectionGraph	Erteilt der GetNetworkConnectionGraph API die Erlaubnis. GetNetworkConnectionGraph akzeptiert eine Eingabeliste mit einer der folgenden IP-Adressen, Server-IDs oder Knoten-IDs. Gibt eine Liste von Knoten und Edges zurück, die dem Kunden helfen, das Netzwerkverbindungsdiagramm zu visualisieren. Diese API wird zur Visualisierung der Netzwerkdiagrammfunktionen in der MigrationHub Konsole verwendet	Lesen			
ListConfigurations	Erteilt der ListConfigurations API die Erlaubnis. ListConfigurations ruft eine Liste von Konfigurationselementen gemäß den Kriterien ab, die Sie in einem Filter angeben. Die Filterkriterien identifizieren die Beziehungsanforderungen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListServerNeighbors	Erteilt der ListServerNeighbors API die Erlaubnis. ListServerNeighbors ruft eine Liste von Servern ab, die einen Netzwerk-Hop von einem angegebenen Server entfernt sind	Auflisten			
StartBatchDeleteConfigurationTask	Erteilt der StartBatchDeleteConfigurationTask API die Erlaubnis. StartBatchDeleteConfigurationTask startet eine asynchrone Batch-Löschung Ihrer Konfigurationselemente. Alle bereitgestellten IDs müssen sich auf denselben Komponententyp (Server, Anwendung, Prozess oder Verbindung) beziehen. Die Ausgabe ist eine eindeutige Aufgaben-ID, mit der Sie den Fortschritt des Löschvorgangs überprüfen können	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartContinuousExport	Erteilt der StartContinuousExport API die Erlaubnis. StartContinuousExport den kontinuierlichen Fluss der vom Agenten erkannten Daten in Amazon Athena starten	Schreiben			iam:AttachRolePolicy iam:CreatePolicy iam:CreateRole iam:CreateServiceLinkedRole
StartDataCollectionByAgentIds	Erteilt der StartDataCollectionByAgentIds API die Erlaubnis. StartDataCollectionByAgentIds weist die angegebenen Agenten oder Connectors an, mit der Datenerfassung zu beginnen	Schreiben			
StartExportTask	Erteilt der StartExportTask API die Erlaubnis. StartExportTask exportiert die Konfigurationsdaten über entdeckte Konfigurationselemente und Beziehungen in einem bestimmten Format in einen S3-Bucket	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartImportTask	Erteilt der StartImportTask API die Erlaubnis. StartImportTask startet eine Importaufgabe. Mit der Migration Hub Hub-Importfunktion können Sie Details Ihrer lokalen Umgebung direkt importieren, AWS ohne die Application Discovery Service (ADS) -Tools wie den Discovery Connector oder Discovery Agent verwenden zu müssen. Dadurch haben Sie die Möglichkeit, die Migrationsbewertung und -planung direkt von Ihren importierten Daten vorzunehmen und Ihre Geräte als Anwendungen zu gruppieren und ihren Migrationsstatus zu verfolgen	Schreiben			discovery:AssociateConfigurationItemsToApplication discovery:CreateApplication discovery:CreateTags discovery:GetDiscoverySummary discovery:ListConfigurations s3:GetObject

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopContinuousExport	Erteilt der StopContinuousExport API die Erlaubnis. StopContinuousExport stoppt den kontinuierlichen Fluss der vom Agenten erkannten Daten zu Amazon Athena	Schreiben			
StopDataCollectionByAgentIds	Erteilt der StopDataCollectionByAgentIds API die Erlaubnis. StopDataCollectionByAgentIds weist die angegebenen Agenten oder Connectors an, die Datenerfassung zu beenden	Schreiben			
UpdateApplication	Erteilt der UpdateApplication API die Erlaubnis. UpdateApplication aktualisiert Metadaten zu einer Anwendung	Schreiben			

Von AWS Application Discovery Service definierte Ressourcentypen

AWS Der Application Discovery Service unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource` Element einer IAM-Richtlinienanweisung. Um den Zugriff auf AWS Application Discovery Service zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

> **Note**
>
> Um den Zugriff zu trennen, erstellen und verwenden Sie separate AWS Konten.

Bedingungsschlüssel für AWS Application Discovery Service

AWS Der Application Discovery Service definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Application Migration Service

AWS Application Migration Service (Servicepräfix: `mgn`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Vom AWS Application Migration Service definierte Aktionen
- Vom AWS Application Migration Service definierte Ressourcentypen
- Bedingungsschlüssel für den AWS Application Migration Service

Vom AWS Application Migration Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ArchiveApplication	Gewährt die Berechtigung zum Archivieren einer Anwendung	Schreiben	ApplicationResource*		
ArchiveWave	Gewährt die Berechtigung zum Archivieren einer Wave	Schreiben	WaveResource*		
AssociateApplications	Gewährt die Berechtigung zum Zuordnen einer Komponente zu einem Wave	Schreiben	ApplicationResource*		
			WaveResource*		
AssociateSourceServers	Gewährt die Berechtigung zum Zuordnen von Quellservern an eine Anwendung	Schreiben	ApplicationResource*		
			SourceServerResource*		
BatchCreateVolumeSnapshotGroupForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer Volume-Snapshot-Gruppe	Schreiben	SourceServerResource*		
BatchDeleteSnapshotRequestF	Gewährt die Berechtigung zum Löschen von Batches von Schnapshot-Anfragen	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
orMgn [nur Berechtigung]					
ChangeServerLifeCycleState	Gewährt die Berechtigung zum Ändern des Lebenszyklusstatus des Quellservers	Schreiben	SourceServerResource*		
CreateApplication	Gewährt die Berechtigung zum Erstellen einer Anwendung	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnector	Gewährt die Berechtigung zum Erstellen eines Konnektors	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLaunchConfigurationTemplate	Gewährt die Berechtigung zum Erstellen einer Startkonfigurationsvorlage	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateReplicationConfigurationTemplate	Gewährt die Berechtigung zum Erstellen einer Replikationskonfigurationsvorlage	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateVcenterClientForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines vcenter-Clients	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWave	Gewährt die Berechtigung zum Erstellen eines Wave	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Gewährt die Berechtigung zum Löschen einer Anwendung	Schreiben	ApplicationResource*		
DeleteConnector	Erteilung der Berechtigung zum Löschen des Verbinders	Schreiben	ConnectorResource*		
DeleteJob	Gewährt die Berechtigung zum Löschen eines Auftrags	Schreiben	JobResource*		
DeleteLaunchConfigurationTemplate	Gewährt die Berechtigung zum Löschen einer Startkonfigurationsvorlage	Schreiben	LaunchConfigurationTemplateResource*		
DeleteReplicationConfigurationTemplate	Gewährt die Berechtigung zum Löschen der Replikationskonfigurationsvorlage	Write	ReplicationConfigurationTemplateResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteSourceServer	Gewährt die Berechtigung zum Löschen des Quellservers	Schreiben	SourceServerResource*		
DeleteVcenterClient	Gewährt die Berechtigung zum Löschen eines vcenter-Clients	Schreiben	VcenterClientResource*		
DeleteWave	Gewährt die Berechtigung zum Löschen eines Wave	Schreiben	WaveResource*		
DescribeJobLogItems	Gewährt die Berechtigung zur Beschreibung von Jobprotokollelementen	Read	JobResource*		
DescribeJobs	Gewährt die Berechtigung zum Beschreiben von Aufträgen	Auflisten			
DescribeLaunchConfigurationTemplates	Gewährt die Berechtigung zur Beschreibung der Startkonfigurationsvorlage	Auflisten			
DescribeReplicationConfigurationTemplates	Gewährt die Berechtigung zur Beschreibung der Replikationskonfigurationsvorlage	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeReplicationServerAssociationsForMgn [nur Berechtigung]	Gewährt die Berechtigung zur Beschreibung von Replikationsservermappingen	Read			
DescribeSnapshotRequestsForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben von Snapshot-Anfragen	Read			
DescribeSourceServers	Gewährt die Berechtigung zur Beschreibung von Quellservern	Auflisten			
DescribeVcenterClients	Gewährt die Berechtigung zum Beschreiben eines vcenter-Clients	Auflisten			
DisassociateApplications	Gewährt die Berechtigung zum Trennen von Anwendungen von einer Wave	Schreiben	ApplicationResource*		
			WaveResource*		
DisassociateSourceServers	Gewährt die Berechtigung zum Trennen von Quellservern von einer Anwendung	Schreiben	ApplicationResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			SourceServerResource*		
DisconnectFromService	Gewährt die Berechtigung zum Trennen des Quellservers vom Service	Schreiben	SourceServerResource*		
FinalizeCutover	Gewährt die Berechtigung zum Fertigstellen von Cutover	Schreiben	SourceServerResource*		
GetAgentCommandForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen des Agent-Befehls	Read	SourceServerResource*		
GetAgentConfirmedResumeInfoForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von durch Agenten bestätigten Resume-Informationen	Read	SourceServerResource*		
GetAgentInstallationAssetsForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Agenteninstallations-Assets	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAgentReplicationInfoForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Informationen zur Agentenreplikation	Read	SourceServerResource*		
GetAgentRuntimeConfigurationForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen der Agent-Laufzeitkonfiguration	Read	SourceServerResource*		
GetAgentSnapshotCreditsForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Snapshots-Guthaben für Agenten	Read	SourceServerResource*		
GetChannelCommandsForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Channel-Befehlen	Read			
GetLaunchConfiguration	Gewährt die Berechtigung zum Abrufen der Startkonfiguration	Read	SourceServerResource*		
GetReplicationConfiguration	Gewährt die Berechtigung zum Abrufen der Replikationskonfiguration	Lesen	SourceServerResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetVcenterClientCommandsForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von vcenter-Client-Befehlen	Lesen	VcenterClientResource*		
InitializeService	Gewährt die Berechtigung zur Initialisierung des Services	Schreiben			iam:AddRoleToInstanceProfile iam:CreateInstanceProfile iam:CreateServiceLinkedRole iam:GetInstanceProfile
IssueClientCertificateForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Ausstellen eines Client-Zertifikats	Schreiben	SourceServerResource		
ListApplications	Gewährt die Berechtigung zum Auflisten von Anwendungszusammenfassungen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListConnectors	Erteilung der Berechtigung zum Auflisten von Verbindern	Lesen			
ListExportErrors	Gewährt die Berechtigung zum Auflisten der Fehler einer Exportaufgabe	Auflisten	ExportResource*		
ListExports	Gewährt die Berechtigung zum Auflisten von Exportaufgaben	Auflisten			
ListImportErrors	Gewährt die Berechtigung zum Auflisten der Fehler einer Importaufgabe	Auflisten	ImportResource*		
ListImports	Gewährt die Berechtigung zum Auflisten von Importaufgaben	Auflisten			
ListManagedAccounts	Gewährt die Berechtigung, verwaltete Konten aufzulisten	Auflisten			
ListSourceServerActions	Gewährt die Berechtigung zum Auflisten von Aktionsdokumenten des Quellservers	Auflisten	SourceServerResource*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen			
ListTemplateActions	Gewährt die Berechtigung zum Auflisten von Aktionsdokumenten für Startkonfigurationsvorlagen	Auflisten	LaunchConfigurationTemplateResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListWaves	Gewährt die Berechtigung zum Auflisten von Wave-Zusammenfassungen	Auflisten			
MarkAsArchived	Gewährt die Berechtigung zum Markieren des Quellservers als archiviert	Schreiben	SourceServerResource*		
NotifyAgentAuthenticationForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Benachrichtigen der Agentenauthentifizierung	Schreiben	SourceServerResource*		
NotifyAgentConnectedForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Benachrichtigen, dass der Agent verbunden ist	Schreiben	SourceServerResource*		
NotifyAgentDisconnectedForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Benachrichtigen, dass der Agent nicht verbunden ist	Schreiben	SourceServerResource*		
NotifyAgentReplicationProgressForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Benachrichtigen des Agentenreplikationsfortschritts	Schreiben	SourceServerResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
NotifyVcenterClientStartedForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Benachrichtigen, dass der vcenter-Client gestartet wurde	Schreiben	VcenterClientResource*		
PauseReplication	Gewährt die Berechtigung, die Replikation anzuhalten	Schreiben	SourceServerResource*		
PutSourceServerAction	Gewährt die Berechtigung zum Speichern des Aktionsdokuments	Schreiben	SourceServerResource*		
PutTemplateAction	Gewährt die Berechtigung zum Ablegen des Aktionsdokuments für die Startkonfigurationsvorlage	Schreiben	LaunchConfigurationTemplateResource*		
RegisterAgentForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Registrieren eines Agenten	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
RemoveSourceServerAction	Gewährt die Berechtigung zum Entfernen des Aktionsdokuments des Quellservers	Schreiben	SourceServerResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RemoveTemplateAction	Gewährt die Berechtigung zum Entfernen des Aktionsdokuments für die Startkonfigurationsvorlage	Schreiben	LaunchConfigurationTemplateResource*		
ResumeReplication	Gewährt die Berechtigung, die Replikation fortzusetzen	Schreiben	SourceServerResource*		
RetryDataReplication	Gewährt die Berechtigung zum Wiederholen der Replikation	Schreiben	SourceServerResource*		
SendAgentLogsForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Senden von Agenten-Protokollen	Schreiben	SourceServerResource*		
SendAgentMetricsForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Senden von Agenten-Metriken	Schreiben	SourceServerResource*		
SendChannelCommandResultForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Senden von Channel-Befehlsergebnissen	Schreiben			
SendClientLogsForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Senden von Client-Protokollen	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SendClientMetricsForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Senden von Client-Metriken	Schreiben			
SendVcenterClientCommandResultForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Senden von vcenter-Client-Befehlsergebnissen	Schreiben	VcenterClientResource*		
SendVcenterClientLogsForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Senden von vcenter-Client-Protokollen	Schreiben	VcenterClientResource*		
SendVcenterClientMetricsForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Senden von vcenter-Client-Metriken	Schreiben	VcenterClientResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartCutover	Gewährt die Berechtigung zum Starten von Cutover	Schreiben	SourceServerResource*		ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateSecurityGroup ec2:CreateSnapshot ec2:CreateTags ec2:CreateVolume

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ec2:DeleteLaunchTemplateVersions ec2:DeleteSnapshot ec2:DeleteVolume ec2:DescribeAccountAttributes ec2:DescribeAvailabilityZones ec2:DescribeImages ec2:DescribeInstanceAttribute ec2:DescribeInstanceStatus

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSnapshots ec2:DescribeSubnets ec2:DescribeVolumes

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ec2:DetachVolume ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:ReportInstanceStatus ec2:RevokeSecurityGroupEgress ec2:RunInstances ec2:StartInstances ec2:StopInstances ec2:TerminateInstances iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					mgn:ListTagsForResource
				aws:RequestTag/${TagKey} aws:TagKeys	
StartExport	Gewährt die Berechtigung zum Starten einer Exportaufgabe	Schreiben			ec2:DescribeLaunchTemplateVersions mgn:DescribeSourceServers mgn:GetLaunchConfiguration mgn:ListApplications mgn:ListWaves s3:PutObject

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartImport	Gewährt die Berechtigung zum Erstellen einer Importaufgabe	Schreiben			ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplateVersions ec2:ModifyLaunchTemplate mgn:DescribeSourceServers mgn:GetLaunchConfiguration mgn:ListApplications mgn:ListWaves mgn:TagResource mgn:UpdateLaunchCo

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					nfiguration s3:PutObject
StartReplication	Gewährt die Berechtigung zum Starten der Replikation	Schreiben	SourceServerResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartTest	Gewährt die Berechtigung zum Starten von Tests	Schreiben	SourceServerResource*		ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateSecurityGroup ec2:CreateSnapshot ec2:CreateTags ec2:CreateVolume

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ec2:DeleteLaunchTemplateVersions ec2:DeleteSnapshot ec2:DeleteVolume ec2:DescribeAccountAttributes ec2:DescribeAvailabilityZones ec2:DescribeImages ec2:DescribeInstanceAttribute ec2:DescribeInstanceStatus

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSnapshots ec2:DescribeSubnets ec2:DescribeVolumes

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ec2:DetachVolume ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:ReportInstanceStatus ec2:RevokeSecurityGroupEgress ec2:RunInstances ec2:StartInstances ec2:StopInstances ec2:TerminateInstances iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					mgn:ListTagsForResource
				aws:RequestTag/${TagKey} aws:TagKeys	
StopReplication	Gewährt die Berechtigung zum Beenden der Replikation	Schreiben	SourceServerResource*		
TagResource	Gewährt die Berechtigung zum Zuordnen eines Ressourcen-Tags.	Markieren	ApplicationResource		
			ConnectorResource		
			JobResource		
			LaunchConfigurationTemplateResource		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			ReplicationConfigurationTemplateResource		
			SourceServerResource		
			VcenterClientResource		
			WaveResource		
				aws:RequestTag/${TagKey} mgn:CreateAction aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TerminateTargetInstances	Gewährt die Berechtigung zum Beenden von Ziel-Instances	Schreiben	SourceServerResource*		ec2:DeleteVolume ec2:DescribeInstances ec2:DescribeVolumes ec2:TerminateInstances
				aws:RequestTag/${TagKey} aws:TagKeys	
UnarchiveApplication	Gewährt die Berechtigung zum Aufheben der Archivierung einer Anwendung	Schreiben	ApplicationResource*		
UnarchiveWave	Gewährt die Berechtigung zum Aufheben der Archivierung einer Wave	Schreiben	WaveResource*		
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Markieren	ApplicationResource		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			ConnectorResource		
			JobResource		
			LaunchConfigurationTemplateResource		
			ReplicationConfigurationTemplateResource		
			SourceServerResource		
			VcenterClientResource		
			WaveResource		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateAgentBacklogForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren des Agenten-Backlog	Schreiben	SourceServerResource*		
UpdateAgentConversionInfoForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren von Agentenkonvertierungsinformationen	Schreiben	SourceServerResource*		
UpdateAgentReplicationInfoForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren von Agentenreplikationsinformationen	Schreiben	SourceServerResource*		
UpdateAgentReplicationProcessStateForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren des Status des Agentenreplikationsprozesses	Schreiben	SourceServerResource*		
UpdateAgentSourcePropertiesForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren von Quelleneigenschaften für Agenten	Schreiben	SourceServerResource*		
UpdateApplication	Gewährt die Berechtigung zum Aktualisieren einer Anwendung	Schreiben	ApplicationResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateConnector	Gewährt die Berechtigung zum Aktualisieren eines Konnektors	Schreiben	ConnectorResource*		
UpdateLaunchConfiguration	Gewährt die Berechtigung zum Aktualisieren einer Startkonfiguration	Schreiben	SourceServerResource*		
UpdateLaunchConfigurationTemplate	Gewährt die Berechtigung zum Aktualisieren einer Startkonfiguration	Schreiben	LaunchConfigurationTemplateResource*		
UpdateReplicationConfiguration	Gewährt die Berechtigung zum Aktualisieren der Replikationskonfiguration	Schreiben	SourceServerResource*		
UpdateReplicationConfigurationTemplate	Gewährt die Berechtigung zum Aktualisieren der Replikationskonfigurationsvorlage	Schreiben	ReplicationConfigurationTemplateResource*		
UpdateSourceServer	Gewährt die Berechtigung zum Aktualisieren des Quellservers	Schreiben	SourceServerResource*		
UpdateSourceServerReplicationType	Gewährt die Berechtigung zum Aktualisieren des Replikationstyps des Quellservers	Schreiben	SourceServerResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateWave	Gewährt die Berechtigung zum Aktualisieren eines Wave	Schreiben	WaveResource*		
VerifyClientRoleForMgn [nur Berechtigung]	Gewährt die Berechtigung zum Verifizieren der Client-Rolle	Lesen			

Vom AWS Application Migration Service definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
JobResource	`arn:${Partition}:mgn:${Region}:${Account}:job/${JobID}`	aws:ResourceTag/${TagKey}
ReplicationConfigurationTemplateResource	`arn:${Partition}:mgn:${Region}:${Account}:replication-configuration-template/${ReplicationConfigurationTemplateID}`	aws:ResourceTag/${TagKey}
LaunchConfiguratio	`arn:${Partition}:mgn:${Region}:${Account}:launch-configuration-template/${LaunchConfigurationTemplateID}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
nTemplateResource		
VcenterClientResource	arn:${Partition}:mgn:${Region}:${Account}:vcenter-client/${VcenterClientID}	aws:ResourceTag/${TagKey}
SourceServerResource	arn:${Partition}:mgn:${Region}:${Account}:source-server/${SourceServerID}	aws:ResourceTag/${TagKey}
ApplicationResource	arn:${Partition}:mgn:${Region}:${Account}:application/${ApplicationID}	aws:ResourceTag/${TagKey}
WaveResource	arn:${Partition}:mgn:${Region}:${Account}:wave/${WaveID}	aws:ResourceTag/${TagKey}
ImportResource	arn:${Partition}:mgn:${Region}:${Account}:import/${ImportID}	aws:ResourceTag/${TagKey}
ExportResource	arn:${Partition}:mgn:${Region}:${Account}:export/${ExportID}	aws:ResourceTag/${TagKey}
ConnectorResource	arn:${Partition}:mgn:${Region}:${Account}:connector/${ConnectorID}	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für den AWS Application Migration Service

AWS Application Migration Service definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüsseln in der Anforderung	ArrayOfString
mgn:CreateAction	Filtert den Zugriff nach Name einer ressourcenerstellenden API-Aktion	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Application Transformation Service

AWS Application Transformation Service (Servicepräfix: `application-transformation`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Vom AWS Application Transformation Service definierte Aktionen
- Von AWS Application Transformation Service definierte Ressourcentypen
- Bedingungsschlüssel für AWS Application Transformation Service

Vom AWS Application Transformation Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetContainerization	Gewährt die Berechtigung zum Abrufen der Details aller Containerisierungsaufträge	Lesen			
GetDeployment	Gewährt die Berechtigung zum Abrufen der Details aller Bereitstellungsaufträge	Lesen			
GetGroupingAssessment	Gewährt die Berechtigung zum Abrufen eines Gruppenbewertungsvorgangs	Lesen			
GetPortingCompatibilityAssessment	Gewährt die Berechtigung zum Abrufen des Portierungskompatibilitätsvorgangs	Lesen			
GetPortingRecommendationAssessment	Gewährt die Berechtigung zum Abrufen eines Portierungsempfehlungsbewertungsvorgangs	Lesen			
GetRuntimeAssessment	Gewährt die Berechtigung zum Abrufen der Details zu einem Laufzeitbewertungsvorgang	Lesen			
PutLogData	Gewährt die Berechtigung zum Übertragen von Protokollen (nur für Clients vorgesehen)	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutMetricData	Gewährt die Berechtigung zum Übertragen von Metrikdaten (nur für Clients vorgesehen)	Schreiben			
StartContainerization	Gewährt die Berechtigung zum Starten eines Containerisierungsauftrags	Schreiben			
StartDeployment	Gewährt die Berechtigung zum Starten eines Bereitstellungsauftrags	Schreiben			
StartGroupingAssessment	Gewährt die Berechtigung zum Starten eines Gruppenbewertungsvorgangs	Schreiben			
StartPortingCompatibilityAssessment	Gewährt die Berechtigung zum Starten des Portierungskompatibilitätsvorgangs	Schreiben			
StartPortingRecommendationAssessment	Gewährt die Berechtigung zum Starten eines Portierungsempfehlungsbewertungsvorgangs	Schreiben			
StartRuntimeAssessment	Gewährt die Berechtigung zum Starten eines Laufzeitbewertungsvorgangs	Schreiben			

Von AWS Application Transformation Service definierte Ressourcentypen

AWS Application Transformation Service unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf AWS Application Transformation Service zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Application Transformation Service

Application Transformation Service umfasst keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon AppStream 2.0

Amazon AppStream 2.0 (Servicepräfix: `appstream`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon AppStream 2.0 definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Associate AppBlockB	Gewährt die Berechtigung, den angegebenen	Schreiben	app-block*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
uilderAppBlock	Anwendungsblock-Builder mit dem Anwendungsblock zu verknüpfen		app-block-builder*		
				aws:ResourceTag/${TagKey}	
AssociateApplicationFleet	Gewährt die Berechtigung zum Zuordnen der angegebenen Anwendung mit der Flotte	Schreiben	application*		
			fleet*		
				aws:ResourceTag/${TagKey}	
AssociateApplicationToEntitlement	Erteilt die Berechtigung zum Verknüpfen der angegebenen Anwendung mit dem angegebenen Anspruch	Schreiben	stack*		
AssociateFleet	Gewährt die Berechtigung zum Verknüpfen der angegebenen Flotte mit dem angegebenen Stack	Write	fleet*		
			stack*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchAssociateUserStack	Gewährt die Berechtigung zum Verknüpfen des angegebenen Benutzers mit den angegebenen Stacks. Benutzer in einem Benutzerpool können keinen Stacks mit Flotten zugewiesen werden, die Mitglied einer Active-Directory-Domain sind.	Write	stack*		
				aws:ResourceTag/${TagKey}	
BatchDisassociateUserStack	Gewährt die Berechtigung zum Aufheben der angegebenen Benutzer aus den angegebenen Stacks	Write	stack*		
				aws:ResourceTag/${TagKey}	
CopyImage	Gewährt die Berechtigung zum Kopieren des angegebenen Images innerhalb derselben Region oder in einer neuen Region im selben AWS-Konto.	Schreiben	image*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAppBlock	Gewährt die Berechtigung zum Erstellen eines Anwendungsblocks. Anwendungsblocks speichern Details über die virtuelle Festplatte, die die Dateien für die Anwendung enthält, in einem S3-Bucket. Es speichert auch das Einrichtungsskript mit Details zum Bereitstellen der virtuellen Festplatte. Anwendungsblocks werden nur für Elastic-Flotten unterstützt	Schreiben		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateAppBlockBuilder	Gewährt die Berechtigung, einen Anwendungsblock-Builder zu erstellen. Ein Anwendungsblock-Builder ist eine virtuelle Maschine, mit der ein Anwendungsblock erstellt werden kann.	Schreiben	app-block-builder*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAppBlockBuilderStreamingURL	Gewährt die Berechtigung, eine URL zu erstellen, über die eine Anwendungsblock-Builder-Streaming-Sitzung gestartet werden kann.	Schreiben	app-block-builder*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateApplication	Gewährt die Berechtigung zum Erstellen einer Anwendung innerhalb eines Kundenkontos. Anwendungen speichern die Details zum Launchen von Anwendungen auf Streaming-Instances. Dies wird nur für Elastic-Flotten unterstützt	Schreiben	app-block*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateDirectoryConfig	Gewährt die Berechtigung zum Erstellen eines Directory Config-Objekts in AppStream 2.0. Dieses Objekt beschreibt die Konfigurationsinformationen, die erforderlich sind, um Flotten und Image Builder mit Microsoft Active Directory-Domains zu verbinden.	Schreiben			
CreateEntitlement	Erteilt die Berechtigung zum Erstellen einer Berechtigung zur Steuerung des Zugriffs auf Anwendungen basierend auf Benutzerattributen	Schreiben	stack*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateFleet	Gewährt die Berechtigung zum Erstellen einer Flotte. Eine Flotte ist eine Gruppe von Streaming-Instances, aus denen Anwendungen gestartet und an Benutzer gestreamt werden.	Write	fleet*		
			image		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateImageBuilder	Gewährt die Berechtigung zum Erstellen eines Image Builders. Ein Image Builder ist eine virtuelle Maschine, mit der ein Image erstellt werden kann.	Write	image*		
			image-builder*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateImageBuilderStreamingURL	Gewährt die Berechtigung zum Erstellen einer URL, über die eine Image Builder Streaming-Sitzung gestartet werden kann.	Write	image-builder*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateStack	Gewährt die Berechtigung zum Erstellen eines Stacks, um mit dem Streaming von Anwendungen an Benutzer zu beginnen. Ein Stack besteht aus einer zugeordneten Flotte, Benutzerzugriffsrichtlinien und Speicherkonfigurationen.	Write	stack*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStreamingURL	Gewährt die Berechtigung zum Erstellen einer temporären URL, über die eine AppStream 2.0 Streaming-Sitzung für den angegebenen Benutzer gestartet werden kann. Mithilfe einer Streaming-URL kann das Streamen getestet werden, ohne dass ein Benutzer eingerichtet werden muss.	Schreiben	fleet*		
			stack*		
				aws:ResourceTag/${TagKey}	
CreateUpdatedImage	Gewährt die Berechtigung, ein vorhandenes Image im Kundenkonto zu aktualisieren	Schreiben	image*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateUsageReportSubscription	Gewährt die Berechtigung zum Erstellen eines Abonnement für Nutzungsberichte. Nutzungsberichte werden täglich aktualisiert.	Write			
CreateUser	Gewährt die Berechtigung zum Erstellen eines neuen Benutzers im Benutzerpool.	Schreiben			
DeleteAppBlock	Gewährt die Berechtigung zum Löschen des angegebenen Anwendungsblocks	Schreiben	app-block*		
				aws:ResourceTag/${TagKey}	
DeleteAppBlockBuilder	Gewährt die Berechtigung, den angegebenen Anwendungsblock-Builder zu löschen und Kapazitäten freizusetzen	Schreiben	app-block-builder*		
				aws:ResourceTag/${TagKey}	
DeleteApplication	Gewährt die Berechtigung zum Löschen der angegebenen Anwendung	Schreiben	application*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteDirectoryConfig	Gewährt die Berechtigung zum Löschen des angegebenen Directory Config-Objekts aus AppStream 2.0. Dieses Objekt beschreibt die Konfigurationsinformationen, die erforderlich sind, um Flotten und Image Builder mit Microsoft Active Directory-Domains zu verbinden.	Schreiben			
DeleteEntitlement	Gewährt die Berechtigung zum Löschen des angegebenen Anspruchs	Schreiben	stack*		
DeleteFleet	Gewährt die Berechtigung zum Löschen der angegebenen Flotte.	Write	fleet*		
				aws:ResourceTag/${TagKey}	
DeleteImage	Gewährt die Berechtigung zum Löschen des angegebenen Images. Ein Image kann nicht gelöscht werden, wenn es verwendet wird.	Write	image*		
				aws:ResourceTag/${TagKey}	
DeleteImageBuilder	Gewährt die Berechtigung zum Löschen des angegebenen Image Builders und Kapazitäten freizusetzen.	Write	image-builder*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteImagePermissions	Gewährt die Berechtigung zum Löschen von Berechtigungen für das angegebene private Image	Write	image*		
				aws:ResourceTag/${TagKey}	
DeleteStack	Gewährt die Berechtigung zum Löschen des angegebenen Stacks. Nachdem der Stack gelöscht ist, steht auch die Streaming-Umgebung der Anwendung, die vom Stack bereitgestellt wird, nicht länger zur Verfügung. Außerdem werden alle Reservierungen des Stack für Streaming-Sitzungen für Anwendungen freigegeben.	Write	stack*		
				aws:ResourceTag/${TagKey}	
DeleteUsageReportSubscription	Gewährt die Berechtigung zum Deaktivieren der Generation von Nutzungsberichten.	Write			
DeleteUser	Gewährt die Berechtigung zum Löschen eines Benutzers aus dem Benutzerpool¨.	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeAppBlockBuilderAppBlockAssociations	Gewährt die Berechtigung, die Zuordnungen abzurufen, die mit dem angegebenen Anwendungsblock-Builder oder Anwendungsblock verknüpft sind	Lesen	app-block		
			app-block-builder		
DescribeAppBlockBuilders	Gewährt die Berechtigung, eine Liste abzurufen, die eine oder mehrere Anwendungsblock-Builder beschreibt, sofern die Namen der Anwendungsblock-Builder angegeben werden. Andernfalls werden alle Anwendungsblock-Builder im Konto beschrieben.	Lesen	app-block-builder		
DescribeAppBlocks	Gewährt die Berechtigung zum Abrufen einer Liste, die eine oder mehrere angegebenen Anwendungsblocks beschreibt, sofern die ARNs des Anwendungsblocks angegeben werden. Andernfalls werden alle Anwendungsblocks im Konto beschrieben	Lesen	app-block		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeApplicationFleetAssociations	Gewährt die Berechtigung zum Abrufen der Zuordnungen, die mit der angegebenen Anwendung oder Flotte verknüpft sind	Lesen	application		
			fleet		
DescribeApplications	Gewährt die Berechtigung zum Abrufen einer Liste, die eine oder mehrere angegebenen Anwendungen beschreibt, sofern die ARNs der Anwendung angegeben werden. Andernfalls werden alle Anwendungen im Konto beschrieben	Lesen	application		
DescribeDirectoryConfigs	Gewährt die Berechtigung zum Abrufen einer Liste, die eine oder mehrere angegebene Directory Config Objekte für AppStream 2.0 beschreibt, sofern die Namen für diese Objekte bereitgestellt werden. Andernfalls werden alle Directory Config-Objekte im Konto beschrieben. Dieses Objekt beschreibt die Konfigurationsinformationen, die erforderlich sind, um Flotten und Image Builder mit Microsoft Active Directory-Domains zu verbinden.	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeEntitlements	Gewährt die Berechtigung zum Abrufen eines oder aller Ansprüche für den angegebenen Stack	Lesen	stack*		
DescribeFleets	Gewährt die Berechtigung zum Abrufen einer Liste, die eine oder mehrere angegebene Flotten beschreibt, sofern die Namen der Flotten angegeben werden. Andernfalls werden alle Flotten im Konto beschrieben.	Read	fleet		
DescribeImageBuilders	Gewährt die Berechtigung zum Abrufen einer Liste, die eine oder mehrere angegebene Image Builder beschreibt, sofern die Namen der Image Builder angegeben werden. Andernfalls werden alle Image Builder im Konto beschrieben.	Read	image-builder		
DescribeImagePermissions	Gewährt die Berechtigung zum Abrufen einer Liste, die Berechtigungen für gemeinsam genutzte AWS-Konto-IDs auf einem privaten Image beschreibt, das sich in Ihrem Besitz befindet.	Read	image*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeImages	Gewährt die Berechtigung zum Abrufen einer Liste, die eine oder mehrere angegebene Images beschreibt, sofern die Namen oder ARNs der Images bereitgestellt werden. Andernfalls werden alle Images im Konto beschrieben.	Read	image		
DescribeSessions	Gewährt die Berechtigung zum Abrufen einer Liste, die die Streaming-Sitzungen für den angegebenen Stack und die angegebene Flotte beschreibt. Wird für den Stack und die Flotte eine Benutzer-ID bereitgestellt, werden nur die Streaming-Sitzungen für diesen Benutzer beschrieben.	Read	fleet* stack*		
DescribeStacks	Gewährt die Berechtigung zum Abrufen einer Liste, die eine oder mehrere angegebene Stacks beschreibt, sofern die Stack-Namen angegeben werden. Andernfalls werden alle Stacks im Konto beschrieben.	Read	stack		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeUsageReportSubscriptions	Gewährt die Berechtigung zum Abrufen einer Liste, die ein oder mehrere Abonnements für Nutzungsberichte beschreibt.	Read			
DescribeUserStackAssociations	Gewährt die Berechtigung zum Abrufen einer Liste, die die UserStackAssociation Objekte beschreibt.	Read	stack		
DescribeUsers	Gewährt die Berechtigung zum Abrufen einer Liste, die die Benutzer im Benutzerpool beschreibt.	Read			
DisableUser	Gewährt die Berechtigung zum Deaktivieren des angegebenen Benutzers im Benutzerpool. Mit dieser Aktion wird der Benutzer nicht gelöscht.	Schreiben			
DisassociateAppBlockBuilderAppBlock	Gewährt die Berechtigung, die Verknüpfung des angegebenen Anwendungsblock-Builders mit dem Anwendungsblock aufzuheben	Schreiben	app-block*		
			app-block-builder*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateApplicationFleet	Gewährt die Berechtigung zum Aufheben der Zuordnung der angegebenen Anwendung von der angegebenen Flotte	Schreiben	application*		
			fleet*		
				aws:ResourceTag/${TagKey}	
DisassociateApplicationFromEntitlement	Gewährt die Berechtigung zum Aufheben der Zuordnung der angegebenen Anwendung aus dem angegebenen Anspruch	Schreiben	stack*		
DisassociateFleet	Gewährt die Berechtigung zum Aufheben der Mapping der angegebenen Flotte vom angegebenen Stack.	Write	fleet*		
			stack*		
				aws:ResourceTag/${TagKey}	
EnableUser	Gewährt die Berechtigung zum Aktivieren eines Benutzers im Benutzerpool.	Write			
ExpireSession	Gewährt die Berechtigung zum sofortigen Anhalten der angegebenen Streaming-Sitzung.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAssociatedFleets	Gewährt die Berechtigung zum Abrufen des Namens der Flotte, die mit dem angegebenen Stack verknüpft ist.	Read	stack*		
ListAssociatedStacks	Gewährt die Berechtigung zum Abrufen des Namens des Stacks, der mit der angegebenen Flotte verknüpft ist.	Lesen	fleet*		
ListEntitledApplications	Gewährt die Berechtigung zum Abrufen der Anwendungen, die dem angegebenen Anspruch zugeordnet sind	Auflisten	stack*		
ListTagsForResource	Gewährt die Berechtigung zum Abrufen einer Liste aller Tags für die angegebene AppStream 2.0-Ressource. Die folgenden Ressourcen können getaggt werden: Image Builder, Images, Flotten und Stacks.	Lesen			
StartAppBlockBuilder	Gewährt die Berechtigung, den angegebenen Anwendungsblock-Builder zu starten	Schreiben	app-block-builder*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartFleet	Gewährt die Berechtigung zum Starten der angegebenen Flotte.	Write	fleet*		
				aws:ResourceTag/${TagKey}	
StartImageBuilder	Gewährt die Berechtigung zum Starten des angegebenen Image Builders.	Schreiben	image-builder*		
				aws:ResourceTag/${TagKey}	
StopAppBlockBuilder	Gewährt die Berechtigung, den angegebenen Anwendungsblock-Builder zu beenden	Schreiben	app-block-builder*		
				aws:ResourceTag/${TagKey}	
StopFleet	Gewährt die Berechtigung zum Anhalten der angegebenen Flotte.	Write	fleet*		
				aws:ResourceTag/${TagKey}	
StopImageBuilder	Gewährt die Berechtigung zum Anhalten des angegebenen Image Builders.	Write	image-builder*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Stream	Gewährt die Berechtigung, durch die sich verbundene Benutzer mit ihren vorhandenen Anmeldeinformationen anmelden und Anwendungen aus dem angegebenen Stack streamen können.	Write	stack*		
				appstream:userId	
TagResource	Gewährt die Berechtigung zum Hinzufügen oder Überschreiben von einem oder mehreren Tags für die angegebene AppStream 2.0-Ressource. Die folgenden Ressourcen können markiert werden: Image Builder, Images, Flotten, Stacks, Anwendungsblöcke und Anwendungen	Markierung	app-block		
			app-block-builder		
			application		
			fleet		
			image		
			image-builder		
			stack		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Mapping ein oder mehrerer Tags aus der angegebenen AppStream 2.0-Ressource.	Markierung	app-block		
			app-block-builder		
			application		
			fleet		
			image		
			image-builder		
			stack		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateAppBlockBuilder	Gewährt die Berechtigung, den angegebenen Anwendungsblock-Builder zu aktualisieren Ein Anwendungsblock-Builder ist eine virtuelle Maschine, mit der ein Anwendungsblock erstellt werden kann.	Schreiben	app-block-builder*		
				aws:ResourceTag/${TagKey}	
UpdateApplication	Gewährt die Berechtigung zum Aktualisieren der angegebenen Felder in der angegebenen Anwendung	Schreiben	application*		
			app-block		
				aws:ResourceTag/${TagKey}	
UpdateDirectoryConfig	Gewährt die Berechtigung zum Aktualisieren des angegebenen Directory Config-Objekts in AppStream 2.0. Dieses Objekt beschreibt die Konfigurationsinformationen, die erforderlich sind, um Flotten und Image Builder mit Microsoft Active Directory-Domains zu verbinden.	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateEntitlement	Gewährt die Berechtigung zum Aktualisieren der angegebenen Felder für den angegebenen Anspruch	Schreiben	stack*		
UpdateFleet	Gewährt die Berechtigung zum Aktualisieren der angegebenen Fleet. Alle Attribute mit Ausnahme des Flottennamens können im Status STOPPED aktualisiert werden.	Write	fleet*		
			image		
				aws:ResourceTag/${TagKey}	
UpdateImagePermissions	Gewährt die Berechtigung zum Hinzufügen oder Aktualisieren von Berechtigungen für das angegebene private Image	Write	image*		
				aws:ResourceTag/${TagKey}	
UpdateStack	Gewährt die Berechtigung zum Aktualisieren der angegebenen Felder im angegebenen Stack.	Write	stack*		
				aws:ResourceTag/${TagKey}	

Von Amazon AppStream 2.0 definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
fleet	`arn:${Partition}:appstream:${Region}:${Account}:fleet/${FleetName}`	aws:ResourceTag/${TagKey}
image	`arn:${Partition}:appstream:${Region}:${Account}:image/${ImageName}`	aws:ResourceTag/${TagKey}
image-builder	`arn:${Partition}:appstream:${Region}:${Account}:image-builder/${ImageBuilderName}`	aws:ResourceTag/${TagKey}
stack	`arn:${Partition}:appstream:${Region}:${Account}:stack/${StackName}`	aws:ResourceTag/${TagKey}
app-block	`arn:${Partition}:appstream:${Region}:${Account}:app-block/${AppBlockName}`	aws:ResourceTag/${TagKey}
application	`arn:${Partition}:appstream:${Region}:${Account}:application/${ApplicationName}`	aws:ResourceTag/${TagKey}
app-block-builder	`arn:${Partition}:appstream:${Region}:${Account}:app-block-builder/${AppBlockBuilderName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon AppStream 2.0

Amazon AppStream 2.0 definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
appstream:userId	Zugriff auf Filter mithilfe der ID des AppStream 2.0-Benutzers	Zeichenfolge
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüsselwertpaaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS AppSync

AWS AppSync (Servicepräfix: `appsync`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS AppSync definierte Aktionen
- Von AWS AppSync definierte Ressourcentypen
- Bedingungsschlüssel für AWS AppSync

Von AWS AppSync definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateApi	Gewährt die Berechtigung zum Anfügen einer GraphQL-API an einen benutzerdefinierten Domänennamen in AppSync	Schreiben	domain*		
AssociateMergedGraphqlApi	Gewährt die Berechtigung zum Verknüpfen einer zusammengeführten API mit einer Quell-API	Schreiben	graphqlapi*		
AssociateSourceGraphqlApi	Gewährt die Berechtigung zum Verknüpfen einer Quell-API mit einer zusammengeführten API	Schreiben	graphqlapi*		
CreateApiCache	Gewährt die Berechtigung zum Erstellen eines API-Caches in AppSync	Schreiben			
CreateApiKey	Gewährt Berechtigungen zum Erstellen eines eindeutigen Schlüssels, den Sie an Kunden verteilen können, die Ihre API ausführen	Schreiben			
CreateDataSource	Gewährt die Berechtigung zum Erstellen einer Datenquelle	Schreiben			
CreateDomainName	Gewährt die Berechtigung zum Erstellen eines benutzerd	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	efinierten Domänennamens in AppSync				
CreateFunction	Gewährt Berechtigungen zum Erstellen eines neuen Function-Objekts	Schreiben			
CreateGraphqlApi	Gewährt die Berechtigung zum Erstellen einer GraphQL-API, die die AppSync Ressource der obersten Ebene ist	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys appsync:Visibility	iam:CreateServiceLinkedRole
CreateResolver	Gewährt die Berechtigung zum Erstellen eines Resolver-Endpunkts. Ein Resolver konvertiert eingehende Anfragen in ein Format, das eine Datenquelle verstehen kann, und er konvertiert die Antworten der Datenquelle in GraphQL	Schreiben			
CreateType	Gewährt die Berechtigung zum Erstellen eines neuen Objekttyps.	Schreiben			
DeleteApiCache	Gewährt die Berechtigung zum Löschen eines API-Caches in AppSync	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteApiKey	Gewährt Berechtigungen zum Löschen eines API-Schlüssels	Schreiben			
DeleteDataSource	Gewährt die Berechtigung zum Löschen einer Datenquelle	Schreiben			
DeleteDomainName	Gewährt die Berechtigung zum Löschen eines benutzerdefinierten Domänennamens in AppSync	Schreiben	domain*		
DeleteFunction	Gewährt die Berechtigung zum Löschen einer Lambda-Funktion	Schreiben			
DeleteGraphqlApi	Gewährt Berechtigungen zum Löschen eines GraphQL-API-Objekts. Dadurch werden auch alle AppSync Ressourcen unter dieser API bereinigt	Schreiben	graphqlapi*		
				aws:ResourceTag/${TagKey}	
DeleteResolver	Gewährt die Berechtigung zum Löschen einer Resolver-Regel	Schreiben			
DeleteResourcePolicy [nur Berechtigung]	Gewährt die Berechtigung zum Entfernen einer Ressourcenrichtlinie	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteType	Gewährt die Berechtigung zum Löschen eines Ereignistyps.	Schreiben			
DisassociateApi	Gewährt die Berechtigung zum Trennen einer GraphQL-API von einem benutzerdefinierten Domänennamen in AppSync	Schreiben	domain*		
DisassociateMergedGraphqlApi	Gewährt die Berechtigung zum Entfernen einer verknüpften Quell-API aus einer zusammengeführten API, die von der Quell-API identifiziert wurde	Schreiben	mergedApiAssociation*		
DisassociateSourceGraphqlApi	Gewährt die Berechtigung zum Entfernen einer verknüpften Quell-API aus einer zusammengeführten API, die von der zusammengeführten API identifiziert wurde	Schreiben	sourceApiAssociation*		
EvaluateCode	Gewährt die Berechtigung zum Auswerten von Code mit einer Laufzeit und einem Kontext	Lesen			
EvaluateMappingTemplate	Erteilung der Berechtigung zur Auswertung der Vorlagenzuordnung	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
FlushApiCache	Gewährt die Berechtigung zum Leeren eines API-Caches in AppSync	Schreiben			
GetApiAssociation	Gewährt die Berechtigung zum Lesen eines benutzerdefinierten Domänennamens – GraphQL-API-Zuordnungsdetails in AppSync	Lesen	domain*		
GetApiCache	Gewährt die Berechtigung zum Lesen von Informationen zu einem API-Cache in AppSync	Lesen			
GetDataSource	Gewährt Berechtigungen zum Abrufen eines DataSource-Objekts	Lesen			
GetDataSourceIntrospection	Gewährt Berechtigungen zum Abrufen einer Datenquellen-Introspektion	Lesen			
GetDomainName	Gewährt die Berechtigung zum Lesen von Informationen zu einem benutzerdefinierten Domänennamen in AppSync	Lesen	domain*		
GetFunction	Gewährt Berechtigungen zum Abrufen eines Function-Objekts	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetGraphqlApi	Gewährt Berechtigungen zum Abrufen eines GraphQL-API-Objekts	Lesen	graphqlapi*		
				aws:ResourceTag/${TagKey}	
GetGraphqlApiEnvironmentVariables	Gewährt die Berechtigung zum Abrufen der Umgebungsvariablen für eine GraphQL-API	Lesen			
GetIntrospectionSchema	Gewährt Berechtigungen zum Abrufen des Introspektionsschemas für eine GraphQL-API	Lesen			
GetResolver	Gewährt Berechtigungen zum Abrufen eines Resolver-Objekts	Lesen			
GetResourcePolicy [nur Berechtigung]	Gewährt die Berechtigung zum Lesen einer Ressourcenrichtlinie	Lesen			
GetSchemaCreationStatus	Gewährt Berechtigungen zum Abrufen des aktuellen Status einer Produktion zum Erstellen eines Schemas	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetSourceApiAssociation	Gewährt die Berechtigung zum Lesen von Informationen über eine zusammengeführte API, die mit einer Quell-API verknüpft ist	Lesen	sourceApiAssociation*		
GetType	Gewährt die Berechtigung zum Abrufen einer Regel	Lesen			
GraphQL	Gewährt Berechtigungen zum Senden einer GraphQL-Abfrage an eine GraphQL-API	Schreiben	field*		
			graphqlapi*		
ListApiKeys	Gewährt Berechtigungen zum Auflisten der API-Schlüssel für eine bestimmte API	Auflisten			
ListDataSources	Gewährt Berechtigungen zum Auflisten der Datenquellen für eine bestimmte API	Auflisten			
ListDomainNames	Gewährt die Berechtigung zum Aufzählen von benutzerdefinierten Domänennamen in AppSync	Auflisten			
ListFunctions	Gewährt Berechtigungen zum Auflisten der Funktionen für eine bestimmte API	Auflisten			
ListGraphqlApis	Gewährt Berechtigungen zum Auflisten Ihrer GraphQL-APIs	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListResolvers	Gewährt Berechtigungen zum Auflisten der Resolver für eine bestimmte API und einen bestimmten Typ	Auflisten			
ListResolversByFunction	Gewährt Berechtigungen zum Auflisten der Resolver, die einer bestimmten Funktion zugeordnet sind	Auflisten			
ListSourceApiAssociations	Gewährt die Berechtigung zum Auflisten von Quell-APIs, die mit einer zusammengeführten API verknüpft sind	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für eine Ressource	Lesen	graphqlapi		
				aws:ResourceTag/${TagKey}	
ListTypes	Gewährt Berechtigungen zum Auflisten der Typen für eine bestimmte API	Auflisten			
ListTypesByAssociation	Gewährt die Berechtigung zum Auflisten der Typen für eine bestimmte Verknüpfung einer zusammengeführten API und einer Quell-API	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutGraphqlApiEnvironmentVariables	Gewährt die Berechtigung zum Aktualisieren der Umgebungsvariablen für eine GraphQL-API	Schreiben			
PutResourcePolicy [nur Berechtigung]	Gewährt die Berechtigung zum Festlegen einer Ressourcenrichtlinie	Schreiben			
SetWebACL	Gewährt Berechtigungen zum Festlegen von Web-ACL	Schreiben			
SourceGraphQL [nur Berechtigung]	Gewährt die Berechtigung zum Senden einer GraphQL-Abfrage an eine Quell-API einer zusammengeführten API	Schreiben	field* graphqlapi*		
StartDataSourceIntrospection	Gewährt Berechtigungen zur Introspektion einer Datenquelle	Schreiben			
StartSchemaCreation	Gewährt Berechtigungen zum Hinzufügen eines neuen Schemas zu Ihrer GraphQL-API. Dieser Vorgang ist asynchron – GetSchemaCreationStatus kann anzeigen, wenn er abgeschlossen ist	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartSchemaMerge	Gewährt die Berechtigung zum Initiieren einer Schemazusammenführung für eine bestimmte zusammengeführte API und verknüpfte Quell-API	Schreiben	sourceApiAssociation*		
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren	graphqlapi*		
			graphqlapi		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Tagging	graphqlapi*		
			graphqlapi		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateApiCache	Gewährt die Berechtigung zum Aktualisieren eines API-Caches in AppSync	Schreiben			
UpdateApiKey	Gewährt Berechtigungen zum Aktualisieren eines API-Schlüssels für eine bestimmte API	Schreiben			
UpdateDataSource	Gewährt die Berechtigung zum Aktualisieren einer Datenquelle	Schreiben			
UpdateDomainName	Gewährt die Berechtigung zum Aktualisieren eines benutzerdefinierten Domänennamens in AppSync	Schreiben	domain*		
UpdateFunction	Gewährt Berechtigungen zum Aktualisieren eines vorhandenen Function-Objekts	Schreiben			
UpdateGraphqlApi	Gewährt Berechtigungen zum Aktualisieren eines GraphQL-API-Objekts	Schreiben	graphqlapi*		iam:CreateServiceLinkedRole
				aws:ResourceTag/${TagKey}	
UpdateResolver	Gewährt die Berechtigung zum Aktualisieren einer Reservierung.	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateSourceApiAssociation	Gewährt die Berechtigung zum Aktualisieren der Verknüpfung einer zusammengeführten API mit einer Quell-API	Schreiben	sourceApiAssociation*		
UpdateType	Gewährt Berechtigungen zum Aktualisieren eines Type-Objekts	Schreiben			

Von AWS AppSync definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
datasource	`arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}/datasources/${DatasourceName}`	
domain	`arn:${Partition}:appsync:${Region}:${Account}:domainnames/${DomainName}`	
graphqlapi	`arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}`	aws:ResourceTag/${TagKey}

Ressource ntypen	ARN	Bedingungsschlüssel
field	`arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}/types/${TypeName}/fields/${FieldName}`	
type	`arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}/types/${TypeName}`	
function	`arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}/functions/${FunctionId}`	
sourceApi Association	`arn:${Partition}:appsync:${Region}:${Account}:apis/${MergedGraphQLAPIId}/sourceApiAssociations/${Associationid}`	
mergedApi Association	`arn:${Partition}:appsync:${Region}:${Account}:apis/${SourceGraphQLAPIId}/mergedApiAssociations/${Associationid}`	

Bedingungsschlüssel für AWS AppSync

AWS AppSync definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
appsync:Visibility	Filtert den Zugriff nach der Sichtbarkeit einer API	String
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tag-Schlüssel-Wert-Paare in der Anforderung	String
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüsselwertpaaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Artifact

AWS Artifact (Dienstpräfix:`artifact`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Artifact definierte Aktionen
- Von AWS Artifact definierte Ressourcentypen
- Bedingungsschlüssel für AWS Artifact

Von AWS Artifact definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptAgreement	Erteilt die Erlaubnis, eine AWS Vereinbarung anzunehmen, die vom Kundenkonto noch nicht akzeptiert wurde	Schreiben	agreement*		
DownloadAgreement	Erteilt die Erlaubnis, eine AWS Vereinbarung, die noch nicht akzeptiert wurde, oder eine Kundenvereinbarung, die vom Kundenkonto akzeptiert wurde, herunterzuladen	Lesen	agreement customer-agreement		
Get	Erteilt die Genehmigung zum Herunterladen eines AWS Compliance-Berichtspakets	Lesen	report-package*		
GetAccountSettings	Erteilt die Berechtigung, die Kontoeinstellungen für Artifact abzurufen	Lesen			
GetReport	Gewährt die Berechtigung zum Herunterladen eines Berichts	Lesen	report*		
GetReportMetadata	Gewährt die Berechtigung zum Herunterladen von Metadaten, die mit einem Bericht verknüpft sind	Lesen	report*		
GetTermForReport	Gewährt die Berechtigung zum Herunterladen eines Begriffs, der mit einem Bericht verknüpft ist	Lesen	report*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListReports	Gewährt die Berechtigung zum Auflisten von Berichten in Ihrem Konto	Auflisten			
PutAccountSettings	Erteilt die Berechtigung, die Kontoeinstellungen für Artifact festzulegen	Schreiben			
TerminateAgreement	Gewährt die Berechtigung zum Beenden eines Kundenvertrags, der zuvor vom Kundenkonto akzeptiert wurde	Schreiben	customer-agreement*		

Von AWS Artifact definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
report-package	`arn:${Partition}:artifact:::report-package/*`	
customer-agreement	`arn:${Partition}:artifact::${Account}:customer-agreement/*`	

Ressourcentypen	ARN	Bedingungsschlüssel
agreement	`arn:${Partition}:artifact:::agreement/*`	
report	`arn:${Partition}:artifact:${Region}::report/${ReportId}:${Version}`	

Bedingungsschlüssel für AWS Artifact

AWS Artifact definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
artifact:ReportCategory	Filtert den Zugriff nach den Kategorien, denen Berichte zugeordnet sind	String
artifact:ReportSeries	Filtert den Zugriff nach den Serien, denen Berichte zugeordnet sind	String

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Athena

Amazon Athena (Servicepräfix: `athena`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.

- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Athena definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetNamedQuery	Gewährt die Berechtigung zum Abrufen von Informationen zu einzelnen oder mehreren benannten Abfragen	Lesen	workgroup*		
BatchGetPreparedStatement	Erteilung der Erlaubnis, Informationen über eine oder mehrere vorbereitete Aussagen zu erhalten	Lesen	workgroup*		
BatchGetQueryExecution	Gewährt die Berechtigung zum Abrufen von Informationen zu einzelnen oder mehreren Abfrageausführungen	Lesen	workgroup*		
CancelCapacityReservation	Gewährt die Berechtigung zum Widerrufen einer Kapazitätsreservierung	Schreiben	capacity-reservation*		
CancelQueryExecution	Gewährt die Berechtigung zum Abbrechen einer	Schreiben	workgroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Abfrageausführung. Als veraltet gekennzeichnet. Gilt nur für AWS-Services und -Prinzipale, die einen Athena-JDBC-Treiber vor Version 1.1.0 nutzen. Verwenden Sie andernfalls StopQuery Execution.				
CreateCapacityReservation	Gewährt die Berechtigung zum Erstellen einer Kapazitätsreservierung	Schreiben	capacity-reservation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataCatalog	Gewährt die Berechtigung zum Erstellen eines Datenkatalogs	Schreiben	datacatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNamedQuery	Gewährt die Berechtigung zum Erstellen einer benannten Abfrage	Schreiben	workgroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateNotebook	Gewährt die Berechtigung zum Erstellen eines Notebooks	Schreiben	workgroup*		
CreatePreparedStatement	Gewährt die Berechtigung zum Erstellen einer vorbereiteten Anweisung	Schreiben	workgroup*		
CreatePresignedNotebookUrl	Gewährt die Berechtigung zum Erstellen einer vorsignierten Notebook-URL	Schreiben	workgroup*		
CreateWorkGroup	Gewährt die Berechtigung zum Erstellen einer Arbeitsgruppe	Schreiben	workgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCapacityReservation	Gewährt die Berechtigung zum Löschen einer Kapazitätsreservierung	Schreiben	capacity-reservation*		
DeleteDataCatalog	Gewährt die Berechtigung zum Löschen eines Datenkatalogs	Schreiben	datacatalog*		
DeleteNamedQuery	Gewährt die Berechtigung zum Löschen einer angegebenen benannten Abfrage	Schreiben	workgroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteNotebook	Gewährt die Berechtigung zum Löschen eines Notebooks	Schreiben	workgroup*		
DeletePreparedStatement	Gewährt die Berechtigung zum Löschen einer angegebenen vorbereiteten Anweisung	Schreiben	workgroup*		
DeleteWorkGroup	Gewährt die Berechtigung zum Löschen einer Arbeitsgruppe	Schreiben	workgroup*		
ExportNotebook	Gewährt die Berechtigung zum Exportieren eines Notebooks	Schreiben	workgroup*		
GetCalculationExecution	Gewährt die Berechtigung zum Abrufen einer Berechtigung	Lesen	workgroup*		
GetCalculationExecutionCode	Gewährt die Berechtigung zum Abrufen eines Berechtigungscodes	Lesen	workgroup*		
GetCalculationExecutionStatus	Gewährt die Berechtigung zum Abrufen eines Berechtigungsstatus	Lesen	workgroup*		
GetCapacityAssignmentConfiguration	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Kapazitätszuweisung für eine Kapazitätsreservierung	Lesen	capacity-reservation*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetCapacityReservation	Gewährt die Berechtigung zum Abrufen einer Kapazitätsreservierung	Lesen	capacity-reservation*		
GetCatalogs	Gewährt die Berechtigungen zum Zugreifen auf Datenbanken und Tabellen. Gilt nur für von AWS-Services verwaltete Richtlinien und Prinzipale, die einen Athena-JDBC-Treiber der Version 1.1.0 nutzen.	Lesen			
GetDataCatalog	Gewährt die Berechtigung zum Abrufen eines Datenkatalogs	Lesen	datacatalog*		
GetDatabase	Gewährt die Berechtigung zum Abrufen einer Datenbank für einen bestimmten Datenkatalog	Lesen	datacatalog*		
GetExecutionEngine	Gewährt die Berechtigung zum Zugreifen auf die angegebene Datenbank und Tabelle. Gilt nur für von AWS-Services verwaltete Richtlinien und Prinzipale, die einen Athena-JDBC-Treiber der Version 1.1.0 nutzen.	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetExecutionEngines	Gewährt die Berechtigungen zum Zugreifen auf Datenbanken und Tabellen. Gilt nur für von AWS-Services verwaltete Richtlinien und Prinzipale, die einen Athena-JDBC-Treiber der Version 1.1.0 nutzen.	Lesen			
GetNamedQuery	Gewährt die Berechtigung zum Abrufen von Informationen zur angegebenen benannten Abfrage	Lesen	workgroup *		
GetNamespace	Gewährt die Berechtigung zum Zugreifen auf die angegebene Datenbank und Tabelle. Gilt nur für von AWS-Services verwaltete Richtlinien und Prinzipale, die einen Athena-JDBC-Treiber der Version 1.1.0 nutzen.	Lesen			
GetNamespaces	Gewährt die Berechtigungen zum Zugreifen auf Datenbanken und Tabellen. Gilt nur für von AWS-Services verwaltete Richtlinien und Prinzipale, die einen Athena-JDBC-Treiber der Version 1.1.0 nutzen.	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetNotebookMetadata	Gewährt die Berechtigung zum Abrufen von Notebook-Metadaten	Lesen	workgroup*		
GetPreparedStatement	Gewährt die Berechtigung zum Abrufen von Informationen zur angegebenen vorbereiteten Anweisung	Lesen	workgroup*		
GetQueryExecution	Gewährt die Berechtigung zum Abrufen von Informationen zur angegebenen Abfrageausführung	Lesen	workgroup*		
GetQueryExecutions	Gewährt die Berechtigung zum Abrufen von Abfrageausführungen. Als veraltet gekennzeichnet. Gilt nur für AWS-Services und -Prinzipale, die einen Athena-JDBC-Treiber vor Version 1.1.0 nutzen. Verwenden Sie andernfalls ListQueryExecutions.	Lesen			
GetQueryResults	Gewährt die Berechtigung zum Abrufen der Abfrageergebnisse	Lesen	workgroup*		
GetQueryResultsStream	Gewährt die Berechtigung zum Abrufen des Abfrageergebnis-Streams	Lesen	workgroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetQueryRuntimeStatistics	Erteilung der Berechtigung zum Abrufen von Laufzeitstatistiken für die angegebene Abfrageausführung	Lesen	workgroup*		
GetSession	Gewährt die Berechtigung zum Abrufen einer Sitzung	Lesen	workgroup*		
GetSessionStatus	Gewährt die Berechtigung zum Abrufen eines Sitzungsstatus	Lesen	workgroup*		
GetTable	Gewährt die Berechtigung zum Zugreifen auf die angegebene Tabelle. Gilt nur für von AWS-Services verwaltete Richtlinien und Prinzipale, die einen Athena-JDBC-Treiber der Version 1.1.0 nutzen.	Lesen			
GetTableMetadata	Gewährt die Berechtigung zum Abrufen von Metadaten zu einer Tabelle für einen bestimmten Datenkatalog	Lesen	datacatalog*		
GetTables	Gewährt die Berechtigung zum Zugreifen auf Tabellen. Gilt nur für von AWS-Services verwaltete Richtlinien und Prinzipale, die einen Athena-JDBC-Treiber der Version 1.1.0 nutzen.	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetWorkGroup	Gewährt die Berechtigung zum Abrufen einer Arbeitsgruppe	Lesen	workgroup*		
ImportNotebook	Gewährt die Berechtigung zum Importieren eines Notebooks	Schreiben	workgroup*		
ListApplicationDPUSizes	Gewährt die Berechtigung zum Zurückgeben einer Liste von ApplicationRuntimeIds	Auflisten			
ListCalculationExecutions	Gewährt die Berechtigung zum Zurückgeben einer Liste von Berechnungen	Auflisten	workgroup*		
ListCapacityReservations	Gewährt die Berechtigung zum Zurückgeben einer Liste der Kapazitätsreservierungen für das angegebene AWS-Konto	Auflisten			
ListDataCatalogs	Gewährt die Berechtigung zum Zurückgeben einer Liste von Datenkatalogen für das angegebene AWS-Konto	Auflisten			
ListDatabases	Gewährt die Berechtigung zum Zurückgeben einer Liste von Datenbanken für einen bestimmten Datenkatalog	Auflisten	datacatalog*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListEngineVersions	Gewährt die Berechtigung zum Zurückgeben einer Liste von Athena-Engine-Versionen für das angegebene AWS-Konto	Lesen			
ListExecutors	Gewährt die Berechtigung zum Zurückgeben einer Liste von Executors	Auflisten			
ListNamedQueries	Gewährt die Berechtigung zum Zurückgeben einer Liste benannter Abfragen in Amazon Athena für das angegebene AWS-Konto	Auflisten	workgroup *		
ListNotebookMetadata	Gewährt die Berechtigung zum Zurückgeben einer Liste von Notizbüchern für eine bestimmte Arbeitsgruppe	Auflisten	workgroup *		
ListNotebookSessions	Gewährt die Berechtigung zum Zurückgeben einer Liste von Sitzungen für ein bestimmtes Notebook	Auflisten	workgroup *		
ListPreparedStatements	Gewährt die Berechtigung zum Zurückgeben einer Liste von vorbereiteten Anweisungen für das angegebene Arbeitsgruppe	Auflisten	workgroup *		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListQueryExecutions	Gewährt die Berechtigung zum Zurückgeben einer Liste von Abfrageausführungen für das angegebene AWS-Konto	Lesen	workgroup*		
ListSessions	Gewährt die Berechtigung zum Zurückgeben einer Liste der Sitzungen für eine Arbeitsgruppe	Auflisten	workgroup*		
ListTableMetadata	Gewährt die Berechtigung zum Zurückgeben einer Liste von Tabellenmetadaten in einer Datenbank für einen bestimmten Datenkatalog	Lesen	datacatalog*		
ListTagsForResource	Gewährt Berechtigungen zum Zurückgeben einer Liste der Tags für eine Ressource	Lesen	capacity-reservation*		
			datacatalog*		
			workgroup*		
ListWorkGroups	Gewährt die Berechtigung zum Zurückgeben einer Liste von Arbeitsgruppen für das angegebene AWS-Konto	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutCapacityAssignmentConfiguration	Gewährt die Berechtigung, Kapazität aus einer Kapazitätsreservierung Abfragen zuzuweisen	Schreiben	capacity-reservation*		
			workgroup*		
RunQuery	Gewährt die Berechtigung zum Ausführen einer Abfrage Als veraltet gekennzeichnet. Gilt nur für AWS-Services und -Prinzipale, die einen Athena-JDBC-Treiber vor Version 1.1.0 nutzen. Verwenden Sie andernfalls StartQueryExecution.	Schreiben			
StartCalculationExecution	Gewährt die Berechtigung zum Starten einer Berechnungs-Ausführung	Schreiben	workgroup*		
StartQueryExecution	Gewährt die Berechtigung zum Starten einer Abfrageausführung unter Verwendung einer als Zeichenfolge bereitgestellten SQL-Abfrage	Schreiben	workgroup*		
StartSession	Gewährt die Berechtigung zum Starten einer Sitzung	Schreiben	workgroup*		
StopCalculationExecution	Gewährt die Berechtigung zum Stoppen einer Berechnungs-Ausführung	Schreiben	workgroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopQueryExecution	Gewährt die Berechtigung zum Stoppen der angegebenen Abfrageausführung	Schreiben	workgroup*		
TagResource	Gewährt die Berechtigung zum Hinzufügen eines Tags zu einer Ressource	Markierung	capacity-reservation*		
			datacatalog*		
			workgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TerminateSession	Gewährt die Berechtigung zum Beenden einer Sitzung	Schreiben	workgroup*		
UntagResource	Gewährt die Berechtigung zum Entfernen eines Tags von einer Ressource	Markierung	capacity-reservation*		
			datacatalog*		
			workgroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
UpdateCapacityReservation	Gewährt die Berechtigung zum Aktualisieren einer Kapazitätsreservierung.	Schreiben	capacity-reservation*		
UpdateDataCatalog	Gewährt die Berechtigung zum Aktualisieren eines Datenkatalogs	Schreiben	datacatalog*		
UpdateNamedQuery	Gewährt die Berechtigung zum Aktualisieren einer angegebenen benannten Abfrage	Schreiben	workgroup*		
UpdateNotebook	Gewährt die Berechtigung zum Aktualisieren eines Notebooks	Schreiben	workgroup*		
UpdateNotebookMetadata	Gewährt die Berechtigung zum Aktualisieren von Notebook-Metadaten	Schreiben	workgroup*		
UpdatePreparedStatement	Gewährt die Berechtigung zum Aktualisieren einer vorbereiteten Anweisung	Schreiben	workgroup*		
UpdateWorkGroup	Gewährt die Berechtigung zum Aktualisieren einer Arbeitsgruppe	Schreiben	workgroup*		

Von Amazon Athena definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
datacatalog	`arn:${Partition}:athena:${Region}:${Account}:datacatalog/${DataCatalogName}`	aws:ResourceTag/${TagKey}
workgroup	`arn:${Partition}:athena:${Region}:${Account}:workgroup/${WorkGroupName}`	aws:ResourceTag/${TagKey}
capacity-reservation	`arn:${Partition}:athena:${Region}:${Account}:capacity-reservation/${CapacityReservationName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Athena

Amazon Athena definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüsselwertpaaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Audit Manager

AWS Audit Manager (Servicepräfix: `auditmanager`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Vom AWS Audit Manager definierte Aktionen
- Von AWS Audit Manager definierte Ressourcentypen
- Bedingungsschlüssel für AWS Audit Manager

Vom AWS Audit Manager definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen.

Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateAssessmentReportEvidenceFolder	Gewährt die Berechtigung, einen Beweisordner mit einem Bewertungsbericht in AWS Audit Manager zu verknüpfen	Write	assessment*		
BatchAssociateAssessmentReportEvidence	Gewährt die Berechtigung, eine Beweisliste mit einem Bewertungsbericht in AWS Audit Manager zu verknüpfen	Write	assessment*		
BatchCreateDelegationByAssessment	Gewährt die Berechtigung, Delegierungen für eine Bewertung in AWS Audit Manager zu erstellen	Write	assessment*		
BatchDeleteDelegationByAssessment	Gewährt die Berechtigung, Delegierungen für eine Bewertung in AWS Audit Manager zu löschen	Write	assessment*		
BatchDisassociateAssessmentReportEvidence	Gewährt die Berechtigung, die Verknüpfung einer Beweisliste mit einem Bewertungsbericht in AWS Audit Manager zu trennen	Write	assessment*		
BatchImportEvidenceToAssessmentControl	Gewährt die Berechtigung, eine Beweisliste in eine Bewertungskontrolle in AWS Audit Manager zu importieren	Write	assessmentControlSet*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAssessment	Gewährt die Berechtigung, eine Bewertung zur Verwendung mit AWS Audit Manager zu erstellen	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssessmentFramework	Gewährt die Berechtigung zum Erstellen eines Frameworks zur Verwendung in AWS Audit Manager	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssessmentReport	Gewährt die Berechtigung, einen Bewertungsbericht in AWS Audit Manager zu erstellen	Write	assessment*		
CreateControl	Gewährt die Berechtigung zum Erstellen einer Kontrolle zur Verwendung in AWS Audit Manager	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAssessment	Gewährt die Berechtigung zum Löschen einer Bewertung in AWS Audit Manager	Write	assessment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAssessmentFramework	Gewährt die Berechtigung zum Löschen eines Bewertungs-Frameworks in AWS Audit Manager	Schreiben	assessmentFramework*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAssessmentFrameworkShare	Gewährt die Berechtigung zum Löschen einer Freigabeanforderung für ein benutzerdefiniertes Framework in AWS Audit Manager	Schreiben			
DeleteAssessmentReport	Gewährt die Berechtigung zum Löschen eines Bewertungsberichts in AWS Audit Manager	Write	assessment*		
DeleteControl	Gewährt die Berechtigung zum Löschen einer Kontrolle in AWS Audit Manager	Write	control*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
DeregisterAccount	Gewährt die Berechtigung zum Aufheben der Registrierung eines Kontos in AWS Audit Manager	Write			
DeregisterOrganizationAdminAccount	Gewährt die Berechtigung zum Aufheben der Registrierung des delegierten Administratorkontos für AWS Audit Manager	Write			
DisassociateAssessmentReportEvidenceFolder	Gewährt die Berechtigung, die Verknüpfung eines Beweisordners mit einem Bewertungsbericht in AWS Audit Manager zu trennen	Write	assessment*		
GetAccountStatus	Gewährt die Berechtigung zum Abrufen des Status eines Kontos in AWS Audit Manager	Read			
GetAssessment	Gewährt die Berechtigung zum Abrufen einer Bewertung, die in AWS Audit Manager erstellt wurde	Read	assessment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAssessmentFramework	Gewährt die Berechtigung zum Abrufen eines Bewertungs-Frameworks in AWS Audit Manager	Read	assessmentFramework*		
GetAssessmentReportUrl	Gewährt die Berechtigung zum Abrufen der URL für einen Bewertungsbericht in AWS Audit Manager	Read	assessment*		
GetChangeLogs	Gewährt die Berechtigung, Änderungsprotokolle für eine Bewertung in AWS Audit Manager abzurufen	Read	assessment*		
GetControl	Gewährt die Berechtigung zum Abrufen einer Kontrolle in AWS Audit Manager	Read	control*		
GetDelegations	Gewährt die Berechtigung zum Abrufen aller Delegierungen in AWS Audit Manager	List			
GetEvidence	Gewährt die Berechtigung zum Abrufen von Beweisen aus AWS Audit Manager	Read	assessmentControlSet*		
GetEvidenceByEvidenceFolder	Gewährt die Berechtigung zum Abrufen aller Beweise aus einem Beweisordner in AWS Audit Manager	Lesen	assessmentControlSet*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetEvidenceFileUploadUrl	Gewährt die Berechtigung, eine vorsignierte Amazon-S3-URL abzurufen, die verwendet werden kann, um eine Datei als manuellen Beweis hochzuladen	Lesen			
GetEvidenceFolder	Gewährt die Berechtigung zum Abrufen des Beweisordners aus AWS Audit Manager	Read	assessmentControlSet*		
GetEvidenceFoldersByAssessment	Gewährt die Berechtigung zum Abrufen aller Beweisordner aus einer Bewertung in AWS Audit Manager	Read	assessment*		
GetEvidenceFoldersByAssessmentControl	Gewährt die Berechtigung zum Abrufen der Beweisordner aus einer Bewertungskontrolle in AWS Audit Manager	Lesen	assessmentControlSet*		
GetInsights	Gewährt die Berechtigung zum Abrufen von Analytik-Daten für alle aktiven Bewertungen	Lesen			
GetInsightsByAssessment	Gewährt die Berechtigung zum Abrufen von Analytik-Daten für spezifische aktive Bewertungen	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetOrganizationAdminAccount	Gewährt die Berechtigung zum Abrufen des delegierten Administratorkontos in AWS Audit Manager	Read			
GetServicesInScope	Gewährt die Berechtigung zum Abrufen der Services, die bei einer Bewertung in AWS Audit Manager inbegriffen sind	Read			
GetSettings	Gewährt die Berechtigung zum Abrufen aller in AWS Audit Manager konfigurierten Einstellungen	Lesen			
ListAssessmentControlInsightsByControlDomain	Gewährt die Berechtigung, Analytik-Daten für Steuerelemente in einer bestimmten Kontroll-Domain und aktiven Bewertung aufzulisten	Auflisten			
ListAssessmentFrameworkShareRequests	Gewährt die Berechtigung zum Auflisten aller gesendeten oder empfangenen Freigabeanforderungen für benutzerdefinierte Frameworks in AWS Audit Manager	Auflisten			
ListAssessmentFrameworks	Gewährt die Berechtigung zum Auflisten aller Bewertungs-Frameworks in AWS Audit Manager	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAssessmentReports	Gewährt die Berechtigung zum Auflisten aller Bewertungsberichte in AWS Audit Manager	List			
ListAssessments	Gewährt die Berechtigung zum Auflisten aller Bewertungen in AWS Audit Manager	Auflisten			
ListControlDomainInsights	Gewährt die Berechtigung zum Abrufen von Analytik-Daten für Kontrolldomains in allen aktiven Bewertungen	Auflisten			
ListControlDomainInsightsByAssessment	Gewährt die Berechtigung, Analytik-Daten für Kontrolldomains in einer bestimmten aktiven Bewertung aufzulisten	Auflisten			
ListControlInsightsByControlDomain	Gewährt die Berechtigung, Analytik-Daten für Steuerelemente in einer bestimmten Kontroll-Domain in allen aktiven Bewertungen aufzulisten	Auflisten			
ListControls	Gewährt die Berechtigung zum Auflisten aller Kontrollen in AWS Audit Manager	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListKeywordsForDataSource	Gewährt die Berechtigung zum Auflisten aller Datenquellen-Schlüsselwörter in AWS Audit Manager	List			
ListNotifications	Gewährt die Berechtigung zum Auflisten aller Benachrichtigungen in AWS Audit Manager	List			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für eine AWS Audit-Manager-Ressource	Lesen	assessment control		
RegisterAccount	Gewährt die Berechtigung zum Registrieren eines Kontos in AWS Audit Manager	Write			
RegisterOrganizationAdminAccount	Gewährt die Berechtigung zum Registrieren eines Kontos innerhalb der Organisation als delegierter Administrator für AWS Audit Manager	Schreiben			
StartAssessmentFrameworkShare	Gewährt die Berechtigung zum Erstellen einer Freigabeanforderung für ein benutzerdefiniertes Framework in AWS Audit Manager	Schreiben	assessmentFramework*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Markieren einer AWS Audit-Manager-Ressource	Markieren	assessment		
			control		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer AWS Audit-Manager-Ressource	Markieren	assessment		
			control		
				aws:TagKeys	
UpdateAssessment	Gewährt die Berechtigung zum Aktualisieren einer Bewertung in AWS Audit Manager	Write	assessment*		
UpdateAssessmentControl	Gewährt die Berechtigung zum Aktualisieren einer Bewertungskontrolle in AWS Audit Manager	Write	assessmentControlSet*		
UpdateAssessmentControlSetStatus	Gewährt die Berechtigung zum Aktualisieren des Status eines Bewertungskontrollsatzes in AWS Audit Manager	Write	assessmentControlSet*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateAssessmentFramework	Gewährt die Berechtigung zum Aktualisieren eines Bewertungs-Frameworks im AWS Audit Manager	Schreiben	assessmentFramework*		
UpdateAssessmentFrameworkShare	Gewährt die Berechtigung zum Aktualisieren einer Freigabeanforderung für ein benutzerdefiniertes Framework in AWS Audit Manager	Schreiben			
UpdateAssessmentStatus	Gewährt die Berechtigung zum Aktualisieren des Status einer Bewertung in AWS Audit Manager	Write	assessment*		
UpdateControl	Gewährt die Berechtigung zum Aktualisieren einer Kontrolle in AWS Audit Manager	Write	control*		
UpdateSettings	Gewährt die Berechtigung zum Aktualisieren von Einstellungen in AWS Audit Manager	Write			
ValidateAssessmentReportIntegrity	Gewährt die Berechtigung zum Überprüfen der Integrität eines Bewertungsberichts in AWS Audit Manager	Read			

Von AWS Audit Manager definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
assessment	`arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${AssessmentId}`	
assessmentFramework	`arn:${Partition}:auditmanager:${Region}:${Account}:assessmentFramework/${AssessmentFrameworkId}`	
assessmentControlSet	`arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${AssessmentId}/controlSet/${ControlSetId}`	
control	`arn:${Partition}:auditmanager:${Region}:${Account}:control/${ControlId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Audit Manager

AWS Audit Manager definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Auto Scaling

AWS Auto Scaling (Servicepräfix: `autoscaling-plans`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Auto Scaling definierte Aktionen
- Von AWS Auto Scaling definierte Ressourcentypen
- Bedingungsschlüssel für AWS Auto Scaling

Von AWS Auto Scaling definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen.

Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateScalingPlan	Erstellt einen Skalierungsplan	Write			
DeleteScalingPlan	Löscht den angegebenen Skalierungsplan	Write			
DescribeScalingPlanResources	Beschreibt die skalierbaren Ressourcen im angegebenen Skalierungsplan	Read			
DescribeScalingPlans	Beschreibt die angegebenen Skalierungspläne oder alle Skalierungspläne	Read			
GetScalingPlanResourceForecastData	Ruft die Prognosedaten für eine skalierbare Ressource ab	Read			
UpdateScalingPlan	Aktualisiert einen Skalierungsplan	Write			

Von AWS Auto Scaling definierte Ressourcentypen

AWS Auto Scaling unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf AWS Auto Scaling zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Auto Scaling

Auto Scaling besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS B2B Data Interchange

AWS B2B Data Interchange (Servicepräfix: `b2bi`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Durch AWS B2B Data Interchange definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCapability	Gewährt die Berechtigung zum Erstellen einer Fähigkeit	Schreiben	transformer		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePartnership	Gewährt die Berechtigung zum Erstellen einer Partnerschaft	Schreiben	capability*		
			profile*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateProfile	Gewährt die Berechtigung zum Erstellen einer Profilaufgabe	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	
CreateTransformer	Gewährt die Berechtigung zum Erstellen eines Transformators	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteCapability	Gewährt die Berechtigung zum Löschen eines Fähigkeit	Schreiben	capability*		
DeletePartnership	Gewährt die Berechtigung zum Löschen einer Partnerschaft	Schreiben	partnership*		
DeleteProfile	Gewährt die Berechtigung zum Löschen eines Profils	Schreiben	profile*		
DeleteTransformer	Gewährt die Berechtigung zum Löschen eines Transformators	Schreiben	transformer*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetCapability	Gewährt die Berechtigung zum Abrufen einer Fähigkeit	Lesen	capability*		
GetPartnership	Gewährt die Berechtigung zum Abrufen einer Partnerschaft	Lesen	partnership*		
GetProfile	Gewährt die Berechtigung zum Abrufen eines Startprofils	Lesen	profile*		
GetTransformer	Gewährt die Berechtigung zum Abrufen eines Transformators	Lesen	transformer*		
GetTransformerJob	Gewährt die Berechtigung zum Abrufen einer Transformationsaufgabe	Lesen	transformer*		
ListCapabilities	Gewährt die Berechtigung zum Auflisten aller Fähigkeiten	Auflisten			
ListPartnerships	Gewährt die Berechtigung zum Auflisten aller Partnerschaften	Auflisten			
ListProfiles	Gewährt die Berechtigung zum Auflisten aller Profile	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine B2Bi-Ressource	Lesen	capability		
			partnership		
			profile		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transformer		
ListTransformers	Gewährt die Berechtigung zum Auflisten aller Transformatoren	Auflisten			
StartTransformerJob	Gewährt die Berechtigung zum Transformieren eines Dokuments	Schreiben	transformer*		
TagResource	Gewährt die Berechtigung zum Markieren einer B2Bi-Ressource mit Tags	Markierung	capability		
			partnership		
			profile		
			transformer		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestMapping	Gewährt die Berechtigung zum Zuordnen einer Beispieldatei	Schreiben	transformer*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TestParsing	Gewährt die Berechtigung zum Analysieren eines Bearbeitungsdokuments	Schreiben	transformer*		
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer B2Bi-Ressource	Markierung	capability		
			partnership		
			profile		
			transformer		
				aws:TagKeys	
UpdateCapability	Gewährt die Berechtigung zum Aktualisieren einer Fähigkeit	Schreiben	capability*		
			transformer		
UpdatePartnership	Gewährt die Berechtigung zum Aktualisieren einer Partnerschaft	Schreiben	partnership*		
			capability		
UpdateProfile	Gewährt die Berechtigung zum Aktualisieren eines Startprofils	Schreiben	profile*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateTransformer	Gewährt die Berechtigung zum Aktualisieren eines Transformators	Schreiben	transformer*		

Durch AWS B2B Data Interchange definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
profile	`arn:${Partition}:b2bi:${Region}:${Account}:profile/${ResourceId}`	aws:ResourceTag/${TagKey}
capability	`arn:${Partition}:b2bi:${Region}:${Account}:capability/${ResourceId}`	aws:ResourceTag/${TagKey}
partnership	`arn:${Partition}:b2bi:${Region}:${Account}:partnership/${ResourceId}`	aws:ResourceTag/${TagKey}
transformer	`arn:${Partition}:b2bi:${Region}:${Account}:transformer/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS B2B Data Interchange

AWS B2B Data Interchange definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden,

um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Backup

AWS Backup (Servicepräfix: `backup`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Backup definierte Aktionen
- Von AWS Backup definierte Ressourcentypen
- Bedingungsschlüssel für AWS Backup

Von AWS Backup definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelLegalHold	Gewährt die Berechtigung zum Aufheben einer rechtlichen Aufbewahrungspflicht	Schreiben	legalHold*		
CopyFromBackupVault [nur Berechtigung]	Gewährt die Berechtigung zum Kopieren aus einem Sicherungstresor	Write	recoveryPoint*		
				backup:CopyTargets backup:CopyTargetOrgPaths	
CopyIntoBackupVault [nur Berechtigung]	Gewährt die Berechtigung zum Kopieren in einen Sicherungstresor	Write	backupVault*		
				aws:RequestTag/${TagKey}	
CreateBackupPlan	Gewährt die Berechtigung zum Erstellen eines neuen Sicherungsplans	Write	backupPlan*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBackupSelection	Gewährt die Berechtigung zum Erstellen einer neuen	Write	backupPlan*		iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Ressourcenmapping in einem Sicherungsplan				
CreateBackupVault	Gewährt die Berechtigung zum Erstellen eines neuen Sicherungstresors	Schreiben	backupVault*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFramework	Gewährt die Berechtigung zum Erstellen eines neuen Frameworks	Schreiben	framework*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLegalHold	Gewährt die Berechtigung zum Erstellen einer neuen gesetzlichen Aufbewahrungspflicht	Schreiben	legalHold*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateLogicallyAirGappedBackupVault	Gewährt die Berechtigung, einen neuen logischen Sicherungsdatenspeicher zu erstellen, einen logischen Container, in dem Sicherungen gespeichert werden	Schreiben	backupVault*		
				aws:RequestTag/${TagKey} aws:TagKeys backup:MinRetentionDays backup:MaxRetentionDays	
CreateReportPlan	Gewährt die Berechtigung zum Erstellen eines neuen Berichtsplans		reportPlan*		
				aws:RequestTag/${TagKey} aws:TagKeys backup:FrameworkArns	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateRestoreTestingPlan	Gewährt die Berechtigung zum Erstellen eines neuen Wiederherstellungs-Testplans	Schreiben	restoreTestingPlan*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRestoreTestingSelection	Gewährt die Berechtigung zum Erstellen einer neuen Ressourcenmapping in einem Wiederherstellungs-Testplan	Schreiben	restoreTestingPlan*		iam:PassRole
DeleteBackupPlan	Gewährt die Berechtigung zum Löschen eines Sicherungsplans	Write	backupPlan*		
DeleteBackupSelection	Gewährt die Berechtigung zum Löschen einer Ressourcenmapping aus einem Sicherungsplan	Write	backupPlan*		
DeleteBackupVault	Gewährt die Berechtigung zum Löschen eines Sicherungstresors	Write	backupVault*		
DeleteBackupVaultAccessPolicy	Gewährt die Berechtigung zum Löschen der Zugriffsrichtlinie für den Sicherungstresor	Berechtigungsverwaltung	backupVault*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteBackupVaultLockConfiguration	Gewährt die Berechtigung zum Entfernen der Sperrkonfiguration aus einem Sicherungstresor	Schreiben	backupVault*		
DeleteBackupVaultNotifications	Gewährt die Berechtigung zum Entfernen von Benachrichtigungen aus dem Sicherungstresor	Schreiben	backupVault*		
DeleteBackupVaultSharingPolicy [nur Berechtigung]	Erteilt die Berechtigung zum Löschen der Richtlinie für die gemeinsame Nutzung des Sicherungstresors	Berechtigungsverwaltung	backupVault*		
DeleteFramework	Gewährt die Berechtigung zum Löschen eines Frameworks	Schreiben	framework*		
DeleteRecoveryPoint	Gewährt die Berechtigung zum Löschen eines Wiederherstellungspunkts aus einem Sicherungstresor	Schreiben	recoveryPoint*		
DeleteReportPlan	Gewährt die Berechtigung zum Löschen eines Reaktionsplans	Schreiben	reportPlan*		
DeleteRestoreTestingPlan	Gewährt die Berechtigung zum Löschen eines Wiederherstellungs-Testplans	Schreiben	restoreTestingPlan*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteRestoreTestingSelection	Gewährt die Berechtigung zum Löschen einer Ressourcenzuordnung aus einem Wiederherstellungs-Testplan	Schreiben	restoreTestingPlan*		
DescribeBackupJob	Gewährt die Berechtigung zum Beschreiben einer Sicherungsaufgabe	Read			
DescribeBackupVault	Gewährt die Berechtigung zum Beschreiben eines neuen Sicherungstresors mit dem angegebenen Namen	Read	backupVault*		
DescribeCopyJob	Gewährt die Berechtigung zum Beschreiben eines Kopierauftrags	Lesen			
DescribeFramework	Gewährt die Berechtigung zum Beschreiben eines neuen Frameworks mit dem angegebenen Namen	Lesen	framework*		
DescribeGlobalSettings	Gewährt die Berechtigung zum Beschreiben globaler Einstellungen	Read			
DescribeProtectedResource	Gewährt die Berechtigung zum Beschreiben einer geschützten Ressource	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeRecoveryPoint	Gewährt die Berechtigung zum Beschreiben eines Wiederherstellungspunkts	Read	recoveryPoint*		
DescribeRegionSettings	Gewährt die Berechtigung zum Beschreiben von Einstellungen für die Region	Lesen			
DescribeReportJob	Gewährt die Berechtigung zum Beschreiben eines Wiederherstellungsauftrags	Lesen			
DescribeReportPlan	Gewährt die Berechtigung zum Beschreiben eines neuen Sicherungstresors mit dem angegebenen Namen	Lesen	reportPlan*		
DescribeRestoreJob	Gewährt die Berechtigung zum Beschreiben eines Wiederherstellungsauftrags	Read			
DisassociateRecoveryPoint	Gewährt die Berechtigung zum Trennen der Mapping eines Wiederherstellungspunkts von einem Sicherungstresor	Schreiben	recoveryPoint*		
DisassociateRecoveryPointFromParent	Gewährt die Berechtigung zum Trennen eines Wiederherstellungspunkts von seinem übergeordneten Punkt	Schreiben	recoveryPoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ExportBackupPlanTemplate	Gewährt die Berechtigung zum Exportieren eines Sicherungsplans als JSON	Read			
GetBackupPlan	Gewährt die Berechtigung zum Abrufen eines Sicherungsplans	Read	backupPlan*		
GetBackupPlanFromJSON	Gewährt die Berechtigung zum Umwandeln einer JSON in einen Sicherungsplan	Read			
GetBackupPlanFromTemplate	Gewährt die Berechtigung zum Umwandeln einer Vorlage in einen Sicherungsplan	Read			
GetBackupSelection	Gewährt die Berechtigung zum Abrufen einer Sicherungsplan-Ressourcenmapping	Read	backupPlan*		
GetBackupVaultAccessPolicy	Gewährt die Berechtigung zum Abrufen der Zugriffsrichtlinie für den Sicherungstresor	Read	backupVault*		
GetBackupVaultNotifications	Gewährt die Berechtigung zum Abrufen von Sicherungstresor-Benachrichtigungen	Lesen	backupVault*		
GetBackupVaultSharingPolicy [nur Berechtigung]	Erteilt die Berechtigung zum Abrufen der Richtlinie für die gemeinsame Nutzung des Sicherungstresors	Lesen	backupVault*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetLegalHold	Gewährt die Berechtigung zum Erhalten eines rechtlichen Aufbewahrungspflichts	Lesen	legalHold*		
GetRecoveryPointRestoreMetadata	Gewährt die Berechtigung zum Abrufen von Metadaten zur Wiederherstellung des Wiederherstellungspunkts	Lesen	recoveryPoint*		
GetRestoreJobMetadata	Gewährt die Berechtigung zum Abrufen der Wiederherstellungsmetadaten, die mit einem Wiederherstellungsauftrag zugeordnet sind	Lesen			
GetRestoreTestingInferredMetadata	Gewährt die Berechtigung zum Abrufen von abgeleiteten Metadaten, die durch Wiederherstellungstests generiert wurden	Lesen			
GetRestoreTestingPlan	Gewährt die Berechtigung zum Erstellen eines Wiederherstellungs-Testplans	Lesen	restoreTestingPlan*		
GetRestoreTestingSelection	Gewährt die Berechtigung zum Abrufen eines Ressourcenmappings für einen Wiederherstellungs-Testplan	Lesen	restoreTestingPlan*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetSupportedResourceTypes	Gewährt die Berechtigung zum Abrufen unterstützter Ressourcentypen	Lesen			
ListBackupJobSummaries	Gewährt die Berechtigung zum Auflisten von Sicherungsaufgaben-Zusammenfassungen	Auflisten			
ListBackupJobs	Gewährt die Berechtigung zum Auflisten von Sicherungsaufgaben	List			
ListBackupPlanTemplates	Gewährt die Berechtigung zum Auflisten von Sicherungsplanvorlagen, die von AWS Backup bereitgestellt werden	List			
ListBackupPlanVersions	Gewährt die Berechtigung zum Auflisten von Sicherungsplanversionen	Auflisten	backupPlan*		
ListBackupPlans	Gewährt die Berechtigung zum Auflisten von Sicherungsplänen	Auflisten			
ListBackupSelections	Gewährt die Berechtigung zum Auflisten von Ressourcenzuweisungen für einen bestimmten Sicherungsplan	Auflisten	backupPlan*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListBackupVaults	Gewährt die Berechtigung zum Auflisten von Sicherungstresoren.	Auflisten			
ListCopyJobSummaries	Gewährt die Berechtigung zum Auflisten von Kopieraufträgs-Zusammenfassungen	Auflisten			
ListCopyJobs	Gewährt die Berechtigung zum Auflisten von Kopieraufträgen	Auflisten			
ListFrameworks	Gewährt die Berechtigung, Frameworks aufzulisten	Auflisten			
ListLegalHolds	Gewährt die Berechtigung zum Auflisten eines rechtlichen Aufbewahrungspflichts	Auflisten			
ListProtectedResources	Gewährt die Berechtigung zum Auflisten geschützter Ressourcen von AWS Backup	Auflisten			
ListProtectedResourcesByBackupVault	Erteilt die Berechtigung zur Auflistung geschützter Ressourcen in einem Sicherungstresor	Auflisten	backupVault*		
ListRecoveryPointsByBackupVault	Gewährt die Berechtigung zum Auflisten von Wiederherstellungspunkten in einem Sicherungstresor	Auflisten	backupVault*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListRecoveryPointsByLegalHold	Gewährt die Berechtigung zum Auflisten von Wiederherstellungspunkten für eine rechtliche Aufbewahrungspflicht	Auflisten	legalHold*		
ListRecoveryPointsByResource	Gewährt die Berechtigung zum Auflisten von Wiederherstellungspunkten für eine Ressource	Auflisten			
ListReportJobs	Gewährt die Berechtigung zum Auflisten von Aufträgen.	Auflisten			
ListReportPlans	Gewährt die Berechtigung zum Auflisten aller Reaktionspläne	Auflisten			
ListRestoreJobSummaries	Gewährt die Berechtigung zum Auflisten von Wiederherstellungsauftrags-Zusammenfassungen	Auflisten			
ListRestoreJobs	Gewährt die Berechtigung zum Auflisten von Wiederherstellungsaufträgen	Auflisten			
ListRestoreJobsByProtectedResource	Gewährt die Berechtigung zum Auflisten von Wiederherstellungsaufträgen für eine geschützte Ressource	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListRestoreTestingPlans	Gewährt die Berechtigung zum Auflisten aller Wiederherstellungs-Testpläne	Auflisten			
ListRestoreTestingSelections	Gewährt die Berechtigung zum Auflisten von Ressourcenzuweisungen für einen bestimmten Wiederherstellungs-Testplan	Auflisten	restoreTestingPlan*		
ListTags	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Read	backupPlan		
			backupVault		
			framework		
			legalHold		
			recoveryPoint		
			reportPlan		
			restoreTestingPlan		
PutBackupVaultAccessPolicy	Gewährt die Berechtigung zum Hinzufügen einer Zugriffsrichtlinie zum Sicherungstresor	Berechtigungsverwaltung	backupVault*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutBackupVaultLockConfiguration	Gewährt die Berechtigung zum Hinzufügen einer Sperrkonfiguration zu einem Sicherungstresor	Schreiben	backupVault*		
				backup:ChangeableForDays backup:MinRetentionDays backup:MaxRetentionDays	
PutBackupVaultNotifications	Gewährt die Berechtigung zum Hinzufügen eines SNS-Themas zum Sicherungstresor	Schreiben	backupVault*		
PutBackupVaultSharingPolicy [nur Berechtigung]	Erteilt die Berechtigung zum Hinzufügen einer Freigaberichtlinie zum Sicherungstresor	Berechtigungsverwaltung	backupVault*		
PutRestoreValidationResult	Gewährt die Berechtigung zum Ablegen eines Wiederherstellungs-Überprüfungsergebnisses	Schreiben			
StartBackupJob	Gewährt die Berechtigung zum Starten einer neuen Sicherungsaufgabe	Write	backupVault*		iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartCopyJob	Gewährt die Berechtigung zum Kopieren einer Sicherung aus einem Quell-Sicherungstresor in einen Ziel-Sicherungstresor	Schreiben	recoveryPoint*		iam:PassRole
StartReportJob	Gewährt die Berechtigung zum Starten eines neuen Wiederherstellungsauftrags	Schreiben	reportPlan*		
StartRestoreJob	Gewährt die Berechtigung zum Starten eines neuen Wiederherstellungsauftrags	Write	recoveryPoint*		iam:PassRole
StopBackupJob	Gewährt die Berechtigung zum Stoppen einer Sicherungsaufgabe	Write			
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren	backupPlan		
			backupVault		
			framework		
			legalHold		
			recoveryPoint		
			reportPlan		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			restoreTestingPlan		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Markieren	backupPlan		
			backupVault		
			framework		
			legalHold		
			recoveryPoint		
			reportPlan		
			restoreTestingPlan		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateBackupPlan	Gewährt die Berechtigung zum Aktualisieren eines Sicherungsplans	Schreiben	backupPlan*		
UpdateFramework	Gewährt die Berechtigung zum Aktualisieren eines Frameworks	Schreiben	framework*		
UpdateGlobalSettings	Gewährt die Berechtigung zum Aktualisieren der aktuellen globalen Einstellungen für das AWS-Konto	Write			
UpdateRecoveryPointLifecycle	Gewährt die Berechtigung zum Aktualisieren des Lebenszyklus des Wiederherstellungspunkts	Write	recoveryPoint*		
UpdateRegionSettings	Gewährt die Berechtigung zum Aktualisieren der aktuellen Service-Opt-In-Einstellungen für die Region	Schreiben			
UpdateReportPlan	Gewährt die Berechtigung zum Aktualisieren eines Sicherungsplans	Schreiben	reportPlan*		
				backup:FrameworkArns	
UpdateRestoreTestingPlan	Gewährt die Berechtigung zum Aktualisieren eines Wiederherstellungs-Testplans	Schreiben	restoreTestingPlan*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateRestoreTestingSelection	Gewährt die Berechtigung zum Erstellen eines neuen Ressourcenmappings in einem Wiederherstellungs-Testplan	Schreiben	restoreTestingPlan *		iam:PassRole

Von AWS Backup definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
backupVault	`arn:${Partition}:backup:${Region}:${Account}:backup-vault:${BackupVaultName}`	aws:ResourceTag/${TagKey}
backupPlan	`arn:${Partition}:backup:${Region}:${Account}:backup-plan:${BackupPlanId}`	aws:ResourceTag/${TagKey}
recoveryPoint	`arn:${Partition}:${Vendor}:${Region}:*:${ResourceType}:${RecoveryPointId}`	aws:ResourceTag/${TagKey}
framework	`arn:${Partition}:backup:${Region}:${Account}:framework:${FrameworkName}-${FrameworkId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
reportPlan	`arn:${Partition}:backup:${Region}:${Account}:report-plan:${ReportPlanName}-${ReportPlanId}`	aws:ResourceTag/${TagKey}
legalHold	`arn:${Partition}:backup:${Region}:${Account}:legal-hold:${LegalHoldId}`	aws:ResourceTag/${TagKey}
restoreTestingPlan	`arn:${Partition}:backup:${Region}:${Account}:restore-testing-plan:${RestoreTestingPlanName}-${RestoreTestingPlanId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Backup

AWS Backup definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den zulässigen Werten für jeden der Tags	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach dem Vorhandensein verbindlicher Tags in der Anforderung	ArrayOfString

Bedingungsschlüssel	Beschreibung	Typ
backup:ChangeableForDays	Filtert den Zugriff nach dem Wert des ChangeableForDays Parameters	Numerischer Wert
backup:CopyTargetOrgPaths	Filtert den Zugriff nach Organisationseinheit	ArrayOfString
backup:CopyTargets	Filtert den Zugriff anhand des ARNs eines Sicherungstresors	ArrayOfARN
backup:FrameworkArns	Filtert den Zugriff nach Framework-ARNs	ArrayOfARN
backup:MaxRetentionDays	Filtert den Zugriff nach dem Wert des MaxRetentionDays Parameters	Numerischer Wert
backup:MinRetentionDays	Filtert den Zugriff nach dem Wert des MinRetentionDays Parameters	Numerischer Wert

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Backup Gateway

AWS Backup Gateway (Servicepräfix: `backup-gateway`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Backup Gateway definierte Aktionen
- Von AWS Backup Gateway definierte Ressourcentypen
- Bedingungsschlüssel für AWS Backup Gateway

Von AWS Backup Gateway definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateGatewayToServer	Gewährt die Berechtigung für AssociateGatewayToServer	Schreiben	gateway*		
			hypervisor*		
Backup	Gewährt die Berechtigung für Backup	Schreiben	virtualmachine*		
CreateGateway	Gewährt die Berechtigung für CreateGateway	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteGateway	Gewährt die Berechtigung für DeleteGateway	Schreiben	gateway*		
DeleteHypervisor	Gewährt die Berechtigung für DeleteHypervisor	Schreiben	hypervisor*		
DisassociateGatewayFromServer	Gewährt die Berechtigung für DisassociateGatewayFromServer	Schreiben	gateway*		
GetBandwidthRateLimitSchedule	Gewährt die Berechtigung für GetBandwidthRateLimitSchedule	Lesen	gateway*		
GetGateway	Gewährt die Berechtigung für GetGateway	Lesen	gateway*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetHypervisor	Gewährt die Berechtigung für GetHypervisor	Lesen	hypervisor*		
GetHypervisorPropertyMappings	Gewährt die Berechtigung für GetHypervisorPropertyMappings	Lesen	hypervisor*		
GetVirtualMachine	Gewährt die Berechtigung für GetVirtualMachine	Lesen	virtualmachine*		
ImportHypervisorConfiguration	Gewährt die Berechtigung für ImportHypervisorConfiguration	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
ListGateways	Gewährt die Berechtigung für ListGateways	Lesen			
ListHypervisors	Gewährt die Berechtigung für ListHypervisors	Lesen			
ListTagsForResource	Gewährt die Berechtigung für ListTagsForResource	Lesen	gateway		
			hypervisor		
			virtualmachine		
ListVirtualMachines	Gewährt die Berechtigung für ListVirtualMachines	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutBandwidthRateLimitSchedule	Gewährt die Berechtigung für PutBandwidthRateLimitSchedule	Schreiben	gateway*		
PutHypervisorPropertyMappings	Gewährt die Berechtigung für PutHypervisorPropertyMappings	Schreiben	hypervisor*		iam:PassRole
PutMaintenanceStartTime	Gewährt die Berechtigung für PutMaintenanceStartTime	Schreiben	gateway*		
Restore	Gewährt die Berechtigung für Restore	Schreiben	hypervisor*		
StartVirtualMachinesMetadataSync	Gewährt die Berechtigung für StartVirtualMachinesMetadataSync	Schreiben	hypervisor*		iam:PassRole
TagResource	Gewährt die Berechtigung für TagResource	Tagging	gateway		
			hypervisor		
			virtualmachine		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TestHypervisorConfiguration	Gewährt die Berechtigung für TestHypervisorConfiguration	Schreiben	gateway*		
UntagResource	Gewährt die Berechtigung für UntagResource	Tagging	gateway		
			hypervisor		
			virtualmachine		
				aws:TagKeys	
UpdateGatewayInformation	Gewährt die Berechtigung für UpdateGatewayInformation	Schreiben	gateway*		
UpdateGatewaySoftwareNow	Gewährt die Berechtigung für UpdateGatewaySoftwareNow	Schreiben	gateway*		
UpdateHypervisor	Gewährt die Berechtigung für UpdateHypervisor	Schreiben	gateway*		

Von AWS Backup Gateway definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
gateway	`arn:${Partition}:backup-gateway::${Account}:gateway/${GatewayId}`	aws:ResourceTag/${TagKey}
hypervisor	`arn:${Partition}:backup-gateway::${Account}:hypervisor/${HypervisorId}`	aws:ResourceTag/${TagKey}
virtualmachine	`arn:${Partition}:backup-gateway::${Account}:vm/${VirtualmachineId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Backup Gateway

AWS Backup Gateway definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den zulässigen Werten für jeden der Tags	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Tag-Wert, der der Ressource zugeordnet ist	String
aws:TagKeys	Filtert den Zugriff nach dem Vorhandensein verbindlicher Tags in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Backup-Speicher

AWS Backup-Speicher (Servicepräfix: `backup-storage`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Vom AWS Backup-Speicher definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CommitBackupJob [nur Berechtigung]	Gewährt die Berechtigung zum Festschreiben einer Sicherungsaufgabe	Schreiben			
DeleteObjects [nur Berechtigung]	Gewährt die Berechtigung zum Löschen von Objekten	Schreiben			
DescribeBackupJob [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben einer Sicherungsaufgabe	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBaseBackup [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen der Basissicherung	Schreiben			
GetChunk [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Daten von einem Wiederherstellungspunkt für einen Wiederherstellungsauftrag	Schreiben			
GetIncrementalBaseBackup [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen einer inkrementellen Basissicherung	Schreiben			
GetObjectMetadata [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Metadaten von einem Wiederherstellungspunkt für einen Wiederherstellungsauftrag	Schreiben			
ListChunks [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Daten von einem Wiederherstellungspunkt für einen Wiederherstellungsauftrag	Schreiben			
ListObjects [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Daten von einem Wiederherstellungspunkt für einen Wiederherstellungsauftrag	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
MountCapsule [nur Berechtigung]	Ordnet einen KMS-Schlüssel einem Sicherungstresor zu	Schreiben			
NotifyObjectComplete [nur Berechtigung]	Gewährt die Berechtigung zum Markieren von hochgeladenen Daten für einen Backup-Auftrag als abgeschlossen	Schreiben			
PutChunk [nur Berechtigung]	Gewährt die Berechtigung zum Hochladen von Daten auf einen von AWS Backup verwalteten Wiederherstellungspunkt für einen Backup-Auftrag	Schreiben			
PutObject [nur Berechtigung]	Gewährt die Berechtigung zum Einfügen von Objekten	Schreiben			
StartObject [nur Berechtigung]	Gewährt die Berechtigung zum Hochladen von Daten auf einen von AWS Backup verwalteten Wiederherstellungspunkt für einen Backup-Auftrag	Schreiben			
UpdateObjectComplete [nur Berechtigung]	Gewährt die Berechtigung zum vollständigen Aktualisieren des Objekts	Schreiben			

Von AWS Backup-Speicher definierte Ressourcentypen

Der AWS Backup-Speicher unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf den AWS Backup-Speicher zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für den AWS Backup-Speicher

Der Backup-Speicher umfasst keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Batch

AWS Batch (Servicepräfix: `batch`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Batch definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelJob	Gewährt die Berechtigung zum Abbrechen eines Auftrags in einer AWS-Batch-Auftragswarteschlange in Ihrem Konto	Write	job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateComputeEnvironment	Gewährt die Berechtigung zum Erstellen einer AWS-Batch- Computing-Umgebung in Ihrem Konto	Write	compute-environment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateJobQueue	Gewährt die Berechtigung zum Erstellen einer AWS-Batch-Auftragswarteschlange in Ihrem Konto	Schreiben	compute-environment*		
			job-queue*		
			scheduling-policy		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSchedulingPolicy	Gewährt die Berechtigung zum Erstellen einer AWS-Batch-Planungs-Richtlinie in Ihrem Konto	Schreiben	scheduling-policy*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteComputeEnvironment	Gewährt die Berechtigung zum Löschen einer AWS-Batch- Computing-Umgebung in Ihrem Konto	Write	compute-environment*		
DeleteJobQueue	Gewährt die Berechtigung zum Löschen einer AWS-Batch-Auftragswarteschlange in Ihrem Konto	Schreiben	job-queue*		
DeleteSchedulingPolicy	Gewährt die Berechtigung zum Löschen einer AWS-Batch-Planungs-Richtlinie in Ihrem Konto	Schreiben	scheduling-policy*		
DeregisterJobDefinition	Gewährt die Berechtigung zum Aufheben der Registrierung einer AWS-Batch-Auftragsdefinition in Ihrem Konto	Write	job-definition-revision*		
DescribeComputeEnvironments	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer AWS-Batch-Computing-Umgebungen in Ihrem Konto	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeJobDefinitions	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer AWS-Batch-Auftragsdefinitionen in Ihrem Konto	Read			
DescribeJobQueues	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer AWS-Batch-Auftragswarteschlangen in Ihrem Konto	Read			
DescribeJobs	Gewährt die Berechtigung zum Beschreiben einer Liste von AWS-Batchaufträgen in Ihrem Konto	Lesen			
DescribeSchedulingPolicies	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer AWS-Batch-Planungs-Richtlinien in Ihrem Konto	Lesen			
ListJobs	Gewährt die Berechtigung zum Auflisten der Tags einer AWS-Batchressource in Ihrem Konto.	Auflisten			
ListSchedulingPolicies	Gewährt die Berechtigung zum Auflisten von AWS-Batch-Planungs-Richtlinien in Ihrem Konto	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt Berechtigungen zum Auflisten der Tags einer AWS-Batchressource in Ihrem Konto.	Read	compute-environment		
			job		
			job-definition-revision		
			job-queue		
			scheduling-policy		
RegisterJobDefinition	Gewährt die Berechtigung zum Registrieren einer AWS-Batch-Auftragsdefinition in Ihrem Konto	Write	job-definition*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				batch:User batch:Privileged batch:Image batch:LogDriver batch:AWSLogsGroup batch:AWSLogsRegion batch:AWSLogsStreamPrefix batch:AWSLogsCreateGroup batch:EKSServiceAccountName batch:EKSImage	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				batch:EKSRunAsUser batch:EKSRunAsGroup batch:EKSPrivileged aws:RequestTag/${TagKey} aws:TagKeys	
SubmitJob	Gewährt die Berechtigung zum Übermitteln eines AWS-Batchauftrags aus einer Auftragsdefinition in Ihrem Konto	Write	job-definition* job-queue*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys batch:ShareIdentifier batch:EKSImage	
TagResource	Gewährt die Berechtigung zum Markieren einer AWS-Batch-Ressource in Ihrem Konto	Markieren	compute-environment		
			job		
			job-definition-revision		
			job-queue		
			scheduling-policy		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
TerminateJob	Gewährt die Berechtigung zum Beenden eines Auftrags in einer AWS-Batch-Auftragswarteschlange in Ihrem Konto	Write	job*		
UntagResource	Gewährt die Berechtigung, die Markierung einer AWS-Batch-Ressource in Ihrem Konto	Markieren	compute-environment		
			job		
			job-definition-revision		
			job-queue		
			scheduling-policy		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateComputeEnvironment	Gewährt die Berechtigung zum Aktualisieren einer AWS-Batch-Computing-Umgebung in Ihrem Konto	Write	compute-environment*		
UpdateJobQueue	Gewährt die Berechtigung zum Aktualisieren einer AWS-Batch-Auftragswarteschlange in Ihrem Konto	Schreiben	job-queue*		
			compute-environment		
			scheduling-policy		
UpdateSchedulingPolicy	Gewährt die Berechtigung zum Aktualisieren einer AWS-Batch-Planungs-Richtlinie in Ihrem Konto	Schreiben	scheduling-policy*		

Von AWS Batch definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
compute-environment	`arn:${Partition}:batch:${Region}:${Account}:compute-environment/${ComputeEnvironmentName}`	aws:ResourceTag/${TagKey}
job-queue	`arn:${Partition}:batch:${Region}:${Account}:job-queue/${JobQueueName}`	aws:ResourceTag/${TagKey}
job-definition	`arn:${Partition}:batch:${Region}:${Account}:job-definition/${JobDefinitionName}`	
job-definition-revision	`arn:${Partition}:batch:${Region}:${Account}:job-definition/${JobDefinitionName}:${Revision}`	aws:ResourceTag/${TagKey}
job	`arn:${Partition}:batch:${Region}:${Account}:job/${JobId}`	aws:ResourceTag/${TagKey}
scheduling-policy	`arn:${Partition}:batch:${Region}:${Account}:scheduling-policy/${SchedulingPolicyName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Batch

AWS Batch definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString
batch:AWSLogsCreateGroup	Filtert den Zugriff basierend auf dem angegebenen Protokolltreiber, um zu bestimmen, ob die awslogs-Gruppe für die Protokolle erstellt wird	Bool
batch:AWSLogsGroup	Filtert den Zugriff basierend auf der awslogs-Gruppe, in der sich die Protokolle befinden	Zeichenfolge
batch:AWSLogsRegion	Filtert den Zugriff basierend auf der Region, in die die Protokolle gesendet werden	Zeichenfolge
batch:AWSLogsStreamPrefix	Filtert den Zugriff basierend auf dem awslogs-Protokollstream-Präfix	Zeichenfolge
batch:EKSImage	Filtert den Zugriff durch das Image, das zum Starten eines Containers für einen Amazon-EKS-Auftrag verwendet wird	Zeichenfolge
batch:EKSPrivileged	Filtert den Zugriff nach dem angegebenen privilegierten Parameterwert, der bestimmt, ob der Container erhöhte Berechtigungen auf der Host-Container-Instance (ähnlich dem Stammbenutzer) für einen Amazon-EKS-Auftrag erhält	Bool

Bedingungsschlüssel	Beschreibung	Typ
batch:EKSRunAsGroup	Filtert den Zugriff auf die angegebene numerische Gruppen-ID (gid), die zum Starten eines Containers in einem Amazon-EKS-Auftrag verwendet wird	Numerischer Wert
batch:EKSRunAsUser	Filtert den Zugriff auf die numerische ID (uid) des angegebenen Benutzers, die zum Starten eines Containers in einem Amazon-EKS-Auftrag verwendet wird	Numerischer Wert
batch:EKSServiceAccountName	Filtert den Zugriff nach dem Namen des Service-Kontos, das zum Ausführen des Pods für einen Amazon-EKS-Auftrag verwendet wird	Zeichenfolge
batch:Image	Filtert den Zugriff auf das Image, das zum Starten eines Containers verwendet wird	Zeichenfolge
batch:LogDriver	Filtert den Zugriff basierend auf dem Protokolltreiber, der für den Container verwendet wird	Zeichenfolge
batch:Privileged	Filtert den Zugriff basierend auf dem angegebenen privilegierten Parameterwert, der bestimmt, ob dem Container erhöhte Berechtigungen auf der Host-Container-Instance erteilt wird (ähnlich wie der Root-Benutzer)	Bool
batch:ShareIdentifier	Filtert den Zugriff durch den shareIdentifier, der im abgesendeten Auftrag verwendet wird	Zeichenfolge
batch:User	Filtert den Zugriff basierend auf dem Benutzernamen oder der numerischen UID, die innerhalb des Containers verwendet wird	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Bedrock

Amazon Bedrock (Servicepräfix: `bedrock`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Bedrock definierte Aktionen
- Von Amazon Bedrock definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Bedrock

Von Amazon Bedrock definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ApplyGuardrail	Erteilt die Erlaubnis zum Anbringen einer Leitplanke	Lesen	guardrail*		
AssociateAgentKnowledgeBase	Gewährt die Berechtigung zum Verbinden einer Wissensdatenbank mit einem Kundendienstmitarbeiter	Schreiben	agent* knowledge-base*		
AssociateThirdPartyKnowledgeBase [nur Berechtigung]	Gewährt die Berechtigung zum Verwenden der Plattform eines Drittanbieters zum Speichern von Wissensdaten	Schreiben		bedrock:ThirdPartyKnowledgeBaseCredentialsSecretArn	
CreateAgent	Erteilt die Berechtigung zum Erstellen eines neuen Agenten und eines Testagenten-Alias,	Schreiben		aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	der auf die DRAFT-Agenten-Version verweist			aws:TagKeys	
CreateAgentActionGroup	Erteilt die Berechtigung, eine neue Aktionsgruppe in einem vorhandenen Agenten zu erstellen	Schreiben	agent*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAgentAlias	Erteilt die Berechtigung zum Erstellen eines neuen Alias für einen Agenten	Schreiben	agent*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSource	Gewährt die Berechtigung zum Erstellen einer Datenquelle	Schreiben	knowledge-base*		
CreateEvaluationJob	Gewährt die Berechtigung zum Erstellen eines Auftrags für die Evaluierung von Grundlagenmodellen oder benutzerdefinierten Modellen	Schreiben	custom-model*		
			foundation-model*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFoundationModelAgreement	Gewährt die Berechtigung zum Erstellen einer neuen Grundlagenmodellvereinbarung	Schreiben			
CreateGuardrail	Gewährt die Berechtigung zum Erstellen eines neuen Integritätsschutzes	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGuardrailVersion	Gewährt die Berechtigung zum Erstellen einer neuen Integritätsschutzversion	Schreiben	guardrail*		
CreateKnowledgeBase	Gewährt die Berechtigung zum Erstellen einer Wissensdatenbank	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateModelCustomizationJob	Gewährt die Berechtigung zum Erstellen eines Auftrags zum Anpassen des Modells mit Ihren benutzerdefinierten Trainingsdaten	Schreiben	custom-model*		
			foundation-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelEvaluationJob	Gewährt die Berechtigung zum Erstellen eines Auftrags für die Evaluierung von Grundlagenmodellen oder benutzerdefinierten Modellen	Schreiben	custom-model*		
			foundation-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelInvocationJob	Gewährt die Berechtigung zum Erstellen eines Auftrags zum Aufrufen eines neuen Modells	Schreiben	custom-model*		
			foundation-model*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProvisionedModelThroughput	Gewährt die Berechtigung zum Erstellen eines neuen bereitgestellten Modelldurchsatzes	Schreiben	custom-model*		
			foundation-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAgent	Gewährt die Berechtigung zum Löschen eines zuvor erstellten Agents	Schreiben	agent*		
DeleteAgentActionGroup	Gewährt die Berechtigung zum Löschen einer zuvor erstellten actionGroup	Schreiben	agent*		
DeleteAgentAlias	Erteilt die Erlaubnis, eine zu löschen AgentAlias , die Sie zuvor erstellt haben	Schreiben	agent-alias*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteAgentVersion	Gewährt die Berechtigung zum Löschen einer zuvor erstellten Agent Version	Schreiben	agent*		
DeleteCustomModel	Gewährt die Berechtigung zum Löschen eines zuvor erstellten benutzerdefinierten Modells	Schreiben	custom-model*		
DeleteDataSource	Gewährt die Berechtigung zum Löschen einer Datenquelle	Schreiben	knowledge-base*		
DeleteFoundationModelAgreement	Gewährt die Berechtigung zum Löschen einer zuvor erstellten Grundlagenmodellvereinbarung	Schreiben			
DeleteGuardrail	Gewährt die Berechtigung zum Löschen eines Integritätsschutzes oder seiner Version	Schreiben	guardrail*		
DeleteKnowledgeBase	Gewährt die Berechtigung zum Löschen einer Wissensdatenbank	Schreiben	knowledge-base*		
DeleteModelInvocationLoggingConfiguration	Gewährt die Berechtigung zum Löschen einer bestehenden Konfiguration der Aufnahmeprotokollierung	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteProvisionedModelThroughput	Gewährt die Berechtigung zum Löschen eines zuvor erstellten bereitgestellten Modelldurchsatzes	Schreiben	provisioned-model*		
DetectGeneratedContent	Erteilt die Erlaubnis zu erkennen, ob der bereitgestellte Inhalt mit Amazon Bedrock generiert wurde	Lesen	foundation-model*		
DisassociateAgentKnowledgeBase	Gewährt die Berechtigung zum Trennen einer Wissensdatenbank von einem Kundendienstmitarbeiter	Schreiben	agent*		
			knowledge-base*		
GetAgent	Erteilt die Berechtigung zum Abrufen eines vorhandenen Agenten	Lesen	agent*		
GetAgentActionGroup	Erteilt die Berechtigung zum Abrufen einer vorhandenen Aktionsgruppe	Lesen	agent*		
GetAgentAlias	Erteilt die Berechtigung zum Abrufen eines bestehenden Alias	Lesen	agent-alias*		
GetAgentKnowledgeBase	Gewährt die Berechtigung zum Beschreiben einer einem Kundendienstmitarbeiter zugeordneten Wissensdatenbank	Lesen	agent*		
			knowledge-base*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAgentVersion	Erteilt die Berechtigung zum Abrufen einer bestehenden Agenten-Version	Lesen	agent*		
GetCustomModel	Gewährt die Berechtigung zum Abrufen der Eigenschaften, die einem benutzerdefinierten Bedrock-Modell zugeordnet sind, das Sie erstellt haben	Lesen	custom-model*		
GetDataSource	Gewährt die Berechtigung zum Abrufen einer vorhandenen Datenquelle	Lesen	knowledge-base*		
GetEvaluationJob	Erteilt die Erlaubnis, die mit einem Bewertungsauftrag verknüpften Eigenschaften abzurufen. Verwenden Sie diesen Vorgang, um den Status eines Bewertungsauftrags abzurufen	Lesen	evaluation-job*		
GetFoundationModel	Gewährt die Berechtigung zum Abrufen der Eigenschaften, die einem Bedrock-Grundlagenmodell zugeordnet sind	Lesen	foundation-model*		
GetFoundationModelAvailability	Gewährt die Berechtigung zum Abrufen der Verfügbarkeit eines Grundlagenmodells	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetGuardrail	Gewährt die Berechtigung zum Abrufen eines Integritätsschutzes oder seiner Version	Lesen	guardrail*		
GetIngestionJob	Gewährt die Berechtigung zum Abrufen eines bestehenden Aufnahmeauftrags	Lesen	knowledge-base*		
GetKnowledgeBase	Gewährt die Berechtigung zum Abrufen einer vorhandenen Wissensdatenbank	Lesen	knowledge-base*		
GetModelCustomizationJob	Gewährt die Berechtigung zum Abrufen der Eigenschaften, die einem Modellanpassungsauftrag zugeordnet sind Verwenden Sie diesen Vorgang, um den Status eines Auftrags zur Modellanpassung abzurufen.	Lesen	model-customization-job*		
GetModelEvaluationJob	Gewährt die Berechtigung zum Abrufen der Eigenschaften, die einem Modellbewertungsauftrag zugeordnet sind Verwenden Sie diesen Vorgang, um den Status eines Auftrags zur Modellbewertung abzurufen	Lesen	model-evaluation-job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetModelInvocationJob	Gewährt die Berechtigung zum Abrufen eines Auftrags zum Aufrufen eines Modells	Lesen	model-invocation-job*		
GetModelInvocationLoggingConfiguration	Gewährt die Berechtigung zum Abrufen einer bestehenden Konfiguration der Aufnahmeprotokollierung	Lesen			
GetProvisionedModelThroughput	Gewährt die Berechtigung zum Abrufen eines bereitgestellten Modelldurchsatzes	Lesen	provisioned-model*		
GetUseCaseForModelAccess	Gewährt die Berechtigung zum Abrufen eines Anwendungsfalls für den Modellzugriff	Lesen			
InvokeAgent	Erteilt die Berechtigung zum Senden von Benutzereingaben (nur Text) an einen Agenten für Bedrock	Lesen	agent-alias*		
InvokeModel	Gewährt die Berechtigung zum Aufrufen des angegebenen Bedrock-Modells, um mithilfe der im Anforderungstext bereitgestellten Eingabe Inferenzen auszuführen	Lesen	foundation-model* provisioned-model*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
InvokeModelWithResponseStream	Gewährt die Berechtigung zum Aufrufen des angegebenen Bedrock-Modells, um mithilfe der im Anforderungstext bereitgestellten Eingabe mit Streaming-Antwort Inferenzen auszuführen	Lesen	foundation-model*		
			provisioned-model*		
ListAgentActionGroups	Erteilt die Berechtigung, Aktionsgruppen in einem Agenten aufzulisten	Auflisten	agent*		
ListAgentAliases	Erteilt die Berechtigung, Aliase für einen Agenten aufzulisten	Auflisten	agent*		
ListAgentKnowledgeBases	Gewährt die Berechtigung zum Auflisten von Wissensdatenbanken, die einem Kundendienstmitarbeiter zugeordnet sind	Auflisten	agent*		
ListAgentVersions	Erteilt die Berechtigung zum Auflisten bestehender Agenten-Versionen	Auflisten	agent*		
ListAgents	Erteilt die Berechtigung zum Auflisten vorhandener Agenten	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListCustomModels	Gewährt die Berechtigung zum Abrufen einer Liste der von Ihnen erstellten Bedrock-Modelle	Auflisten			
ListDataSources	Gewährt die Berechtigung zum Auflisten vorhandener Datenquellen in einer Wissensdatenbank	Auflisten	knowledge-base*		
ListEvaluationJobs	Erteilt die Erlaubnis, die Liste der von Ihnen eingereichten Bewertungsjobs abzurufen	Auflisten			
ListFoundationModelAgreementOffers	Gewährt die Berechtigung zum Auflisten von Grundlagenmodellvereinbarungsangeboten	Auflisten			
ListFoundationModels	Gewährt die Berechtigung zum Auflisten der Bedrock-Grundlagenmodelle, die Sie verwenden können	Auflisten			
ListGuardrails	Gewährt die Berechtigung zum Auflisten von Integritätsschutz oder deren Versionen	Auflisten	guardrail		
ListIngestionJobs	Gewährt die Berechtigung zum Auflisten von Aufnahmeaufträgen in einer Datenquelle	Auflisten	knowledge-base*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListKnowledgeBases	Gewährt die Berechtigung zum Auflisten vorhandener Wissensdatenbanken	Auflisten			
ListModelCustomizationJobs	Gewährt die Berechtigung zum Abrufen einer Liste der von Ihnen übermittelten Aufträge zur Modellanpassung	Auflisten			
ListModelEvaluationJobs	Gewährt die Berechtigung zum Abrufen einer Liste der von Ihnen übermittelten Aufträge zur Modellbewertung	Auflisten			
ListModelInvocationJobs	Gewährt die Berechtigung zum Auflisten zuvor erstellter Modellaufrufaufträge	Auflisten			
ListProvisionedModelThroughputs	Gewährt die Berechtigung zum Auflisten zuvor erstellter bereitgestellter Modelldurchsätze	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Bedrock-Ressource	Lesen	agent*		
			agent-alias*		
			custom-model*		
			evaluation-job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			guardrail*		
			knowledge-base*		
			model-customization-job*		
			model-evaluation-job*		
			model-invocation-job*		
			provisioned-model*		
PrepareAgent	Gewährt die Berechtigung, einen vorhandenen Agenten auf den Empfang von Laufzeitanforderungen vorzubereiten	Schreiben	agent*		
PutFoundationModelEntitlement	Gewährt die Berechtigung, Zugriff auf ein Grundlagenmodell zu gewähren	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutModelInvocationLoggingConfiguration	Gewährt die Berechtigung zum Löschen einer bestehenden Konfiguration der Aufnahmeprotokollierung	Schreiben			
PutUseCaseForModelAccess	Gewährt die Berechtigung zum Ablegen eines Anwendungsfalls für den Modellzugriff	Schreiben			
Retrieve	Gewährt die Berechtigung zum Abrufen der aufgenommenen Daten aus einer Wissensdatenbank	Lesen	knowledge-base*		
RetrieveAndGenerate	Gewährt die Berechtigung zum Senden von Benutzereingaben zum Abrufen und Generieren	Schreiben			
StartIngestionJob	Gewährt die Berechtigung zum Starten eines Aufnahmeauftrags	Schreiben	knowledge-base*		
StopEvaluationJob	Erteilt die Erlaubnis, eine Evaluierungsaufgabe zu beenden, während sie in Bearbeitung ist	Schreiben	evaluation-job*		
StopModelCustomizationJob	Gewährt die Berechtigung zum Beenden eines Auftrags zur Anpassung eines Bedrock-Modells, während er läuft	Schreiben	model-customization-job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopModelInvocationJob	Gewährt die Berechtigung zum Anhalten eines Auftrags zum Aufrufen eines Modells, den Sie zuvor gestartet haben	Schreiben	model-invocation-job*		
TagResource	Gewährt die Berechtigung zum Markieren einer Bedrock-Ressource mit Tags	Tagging	agent		
			agent-alias		
			custom-model		
			evaluation-job		
			guardrail		
			knowledge-base		
			model-customization-job		
			model-evaluation-job		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			model-invocation-job		
			provisioned-model		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Bedrock-Ressource mit Tags	Tagging	agent		
			agent-alias		
			custom-model		
			evaluation-job		
			guardrail		
			knowledge-base		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			model-customization-job		
			model-evaluation-job		
			model-invocation-job		
			provisioned-model		
				aws:TagKeys	
UpdateAgent	Erteilt die Berechtigung zum Aktualisieren eines vorhandenen Agenten	Schreiben	agent*		
UpdateAgentActionGroup	Erteilt die Berechtigung zum Aktualisieren einer vorhandenen Aktionsgruppe	Schreiben	agent*		
UpdateAgentAlias	Erteilt die Berechtigung, einen bestehenden Alias zu aktualisieren	Schreiben	agent-alias*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateAgentKnowledgeBase	Gewährt die Berechtigung zum Aktualisieren einer einem Kundendienstmitarbeiter zugeordneten Wissensdatenbank	Schreiben	agent*		
			knowledge-base*		
UpdateDataSource	Gewährt die Berechtigung zum Aktualisieren einer Datenquelle	Schreiben	knowledge-base*		
UpdateGuardrail	Gewährt die Berechtigung zum Beschreiben eines Integritätsschutzes	Schreiben	guardrail*		
UpdateKnowledgeBase	Gewährt die Berechtigung zum Aktualisieren einer Wissensdatenbank	Schreiben	knowledge-base*		
UpdateProvisionedModelThroughput	Gewährt die Berechtigung zum Aktualisieren eines zuvor erstellten bereitgestellten Modelldurchsatzes	Schreiben	custom-model*		
			foundation-model*		
			provisioned-model*		

Von Amazon Bedrock definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können.

Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
foundation-model	`arn:${Partition}:bedrock:${Region}::foundation-model/${ResourceId}`	
custom-model	`arn:${Partition}:bedrock:${Region}:${Account}:custom-model/${ResourceId}`	aws:ResourceTag/${TagKey}
provisioned-model	`arn:${Partition}:bedrock:${Region}:${Account}:provisioned-model/${ResourceId}`	aws:ResourceTag/${TagKey}
model-customization-job	`arn:${Partition}:bedrock:${Region}:${Account}:model-customization-job/${ResourceId}`	aws:ResourceTag/${TagKey}
agent	`arn:${Partition}:bedrock:${Region}:${Account}:agent/${AgentId}`	aws:ResourceTag/${TagKey}
agent-alias	`arn:${Partition}:bedrock:${Region}:${Account}:agent-alias/${AgentId}/${AgentAliasId}`	aws:ResourceTag/${TagKey}
knowledge-base	`arn:${Partition}:bedrock:${Region}:${Account}:knowledge-base/${KnowledgeBaseId}`	aws:ResourceTag/${TagKey}
model-evaluation-job	`arn:${Partition}:bedrock:${Region}:${Account}:model-evaluation-job/${ResourceId}`	aws:ResourceTag/${TagKey}
evaluation-job	`arn:${Partition}:bedrock:${Region}:${Account}:evaluation-job/${ResourceId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
model-invocation-job	`arn:${Partition}:bedrock:${Region}:${Account}:model-invocation-job/${JobIdentifier}`	aws:ResourceTag/${TagKey}
guardrail	`arn:${Partition}:bedrock:${Region}:${Account}:guardrail/${GuardrailId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Bedrock

Amazon Bedrock definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Erstellung von Anforderungen basierend auf dem zulässigen Satz von Werten für jedes der obligatorischen Tags	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff durch Aktionen basierend auf dem Tag-Wert, der der Ressource zugeordnet ist	String
aws:TagKeys	Filtert den Zugriff durch das Erstellen von Anfragen basierend auf dem Vorhandensein von obligatorischen Tags in der Anfrage	ArrayOfString
bedrock:ThirdPartyKnowledge	Filtert den Zugriff nach dem SecretArn, der die Anmeldeinformationen der Drittanbieterplattform enthält	ARN

Bedingungsschlüssel	Beschreibung	Typ
BaseCredentialsSecretArn		

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Billing

AWS Billing (Servicepräfix: `billing`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Billing definierte Aktionen
- Von AWS Billing definierte Ressourcentypen
- Bedingungsschlüssel für AWS Billing

Von AWS Billing definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn

die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBillingData [nur Berechtigung]	Gewährt die Berechtigung zum Ausführen von Abfragen zu Abrechnungsinformationen	Lesen			
GetBillingDetails [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen der Rechnungsinformationen für Einzelposten	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBillingNotifications [nur Berechtigung]	Gewährt die Berechtigung zum Einsehen der von AWS gesendeten Benachrichtigungen im Zusammenhang mit den Rechnungsinformationen Ihres Kontos	Lesen			
GetBillingPreferences [nur Berechtigung]	Gewährt die Berechtigung zum Einsehen der Rechnungspräferenzen, wie Reserved Instance, Savings Plans und Teilen von Guthaben	Lesen			
GetContractInformation [nur Berechtigung]	Gewährt die Berechtigung zum Einsehen der Vertragsinformationen des Kontos, einschließlich der Vertragsnummer, der Namen der Endbenutzerorganisationen, der Bestellnummern und ob das Konto für die Betreuung von Kunden des öffentlichen Sektors verwendet wird	Lesen			
GetCredits [nur Berechtigung]	Gewährt die Berechtigung zum Aufrufen des eingelösten Guthabens	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetIAMAccessPreference [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen des Status der Rechnungspräferenz „Allow IAM Access“ (IAM-Zugriff zulassen)	Lesen			
GetSellerOfRecord [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen des standardmäßigen eingetragenen Verkäufers	Lesen			
ListBillingViews [nur Berechtigung]	Gewährt die Berechtigung, Abrechnungsinformationen für Ihre Proforma-Abrechnungsgruppen abzurufen	Lesen			
PutContractInformation [nur Berechtigung]	Gewährt die Berechtigung zum Einrichten der Vertragsinformationen des Kontos, einschließlich der Namen der Endbenutzerorganisationen und ob das Konto für die Betreuung von Kunden des öffentlichen Sektors verwendet wird	Schreiben			
RedeemCredits [nur Berechtigung]	Gewährt die Berechtigung zum Einlösen eines AWS-Guthabens	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateBillingPreferences [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren der Rechnungspräferenzen, wie Reserved Instance, Savings Plans und Teilen von Guthaben	Schreiben			
UpdateIAMAccessPreference [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren der Rechnungspräferenz „Allow IAM Access“ (IAM-Zugriff zulassen)	Schreiben			

Von AWS Billing definierte Ressourcentypen

AWS Billing unterstützt nicht die Angabe eines Ressourcen-ARN im Element `Resource` einer IAM-Richtlinienanweisung. Um den Zugriff auf AWS Billing zuzulassen, geben Sie in Ihrer Richtlinie `"Resource": "*"` an.

Bedingungsschlüssel für AWS Billing

Billing besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Billing und Datenexporte für das Kostenmanagement

AWS Billing und Datenexporte für das Kostenmanagement (Service-Präfix: `bcm-data-exports`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Aktionen, die durch Datenexporte von AWS Billing und Datenexporte für das Kostenmanagement
- Ressourcentypen, die durch AWS Billing und Datenexporte für das Kostenmanagement definiert wurden
- Bedingungsschlüssel für AWS Billing und Datenexporte für das Kostenmanagement

Aktionen, die durch Datenexporte von AWS Billing und Datenexporte für das Kostenmanagement

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateExport	Gewährt die Berechtigung zum Erstellen eines Exports	Schreiben	table*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteExport	Gewährt die Berechtigung zum Löschen eines Exports	Schreiben	export*		
				aws:ResourceTag/${TagKey}	
GetExecution	Gewährt die Berechtigung die Ausführung eines Exports zu veranlassen	Lesen	export*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetExport	Gewährt die Berechtigung zum Abrufen eines Exports	Lesen	export*		
				aws:ResourceTag/${TagKey}	
GetTable	Gewährt die Berechtigung, die Details zu einer Tabelle zu erhalten	Lesen	table*		
ListExecutions	Gewährt die Berechtigung zum Auflisten aller Ausführungen eines Exports	Auflisten	export*		
				aws:ResourceTag/${TagKey}	
ListExports	Gewährt die Berechtigung zum Auflisten aller Exporte	Auflisten			
ListTables	Gewährt die Berechtigung zum Auflisten verfügbarer Tabellen	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen	export*		
				aws:ResourceTag/${TagKey}	
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren	export*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Tagging	export*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateExport	Gewährt die Berechtigung zum Aktualisieren eines Exports	Schreiben	export*		
			table*		
				aws:ResourceTag/${TagKey}	

Ressourcentypen, die durch AWS Billing und Datenexporte für das Kostenmanagement definiert wurden

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der

Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
export	`arn:${Partition}:bcm-data-exports:${Region}:${Account}:export/${Identifier}`	aws:ResourceTag/${TagKey}
table	`arn:${Partition}:bcm-data-exports:${Region}:${Account}:table/${Identifier}`	

Bedingungsschlüssel für AWS Billing und Datenexporte für das Kostenmanagement

AWS Billing und Datenexporte für das Kostenmanagement definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Billing Conductor

AWS Billing Conductor (Servicepräfix: `billingconductor`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Billing Conductor definierte Aktionen
- Von AWS Billing Conductor definierte Ressourcentypen
- Bedingungsschlüssel für AWS Billing Conductor

Von AWS Billing Conductor definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt,

müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Associate Accounts	Gewährt die Berechtigung, einer Abrechnungsgruppe zwischen einem und 30 Konten zuzuordnen	Schreiben	billinggroup*		
Associate PricingRules	Gewährt die Berechtigung zum Zuordnen von Preisregeln	Schreiben	pricingplan*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			pricingrule*		
BatchAssociateResourcesToCustomLineItem	Gewährt die Berechtigung, Ressourcen in einem Batchvorgang mit einem benutzerdefinierten Prozent-Einzelposten zu verknüpfen	Schreiben	customlineitem*		
BatchDisassociateResourcesFromCustomLineItem	Gewährt die Berechtigung, die Verknüpfung von Ressourcen in einem Batchvorgang mit einem benutzerdefinierten Prozent-Einzelposten aufzuheben	Schreiben	customlineitem*		
CreateBillingGroup	Gewährt die Berechtigung zum Erstellen einer Fakturierungsgruppe.	Schreiben	pricingplan*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateCustomLineItem	Gewährt die Berechtigung zum Erstellen eines benutzerdefinierten Einzelpostens	Schreiben	billinggroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePricingPlan	Gewährt die Berechtigung zum Erstellen eines Preisplans	Schreiben	pricingrule*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePricingRule	Gewährt die Berechtigung zum Erstellen einer Preisregel	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteBillingGroup	Gewährt die Berechtigung zum Löschen einer Fakturierungsgruppe	Schreiben	billinggroup*		
DeleteCustomLineItem	Gewährt die Berechtigung zum Löscjen der Details eines benutzerdefinierten Einzelpostens	Schreiben	customlineitem*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeletePricingPlan	Gewährt die Berechtigung zum Löschen eines Preisplans	Schreiben	pricingplan*		
DeletePricingRule	Gewährt die Berechtigung zum Löschen einer Preisregel	Schreiben	pricingrule*		
DisassociateAccounts	Gewährt die Berechtigung, die Zuordnung einer Abrechnungsgruppe zwischen einem und 30 Konten aufzuheben	Schreiben	billinggroup*		
DisassociatePricingRules	Gewährt die Berechtigung, die Zuordnung von Preisregeln aufzuheben	Schreiben	pricingplan* pricingrule*		
GetBillingGroupCostReport	Gewährt die Berechtigung zum Anzeigen des Kostenberichts für Abrechnungsgruppen für die angegebene Abrechnungsgruppe	Lesen	billinggroup*		
ListAccountAssociations	Gewährt die Berechtigung, die verknüpften Konten des Zahlerkontos für den angegebenen Abrechnungszeitraum aufzulisten und gleichzeitig der Abrechnungsgruppe bereitzustellen, zu der die verknüpften Konten gehören	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListBillingGroupCostReports	Gewährt die Berechtigung zum Anzeigen des Kostenberichts für Abrechnungsgruppen	Lesen			
ListBillingGroups	Gewährt die Berechtigung zum Anzeigen der Fakturierungsgruppendetails	Lesen			
ListCustomLineItemVersions	Gewährt die Berechtigung zum Anzeigen von benutzerdefinierten Werbebuchungsversionen	Lesen	customlineitem*		
ListCustomLineItems	Gewährt die Berechtigung zum Anzeigen der Details eines benutzerdefinierten Einzelpostens	Lesen			
ListPricingPlans	Gewährt die Berechtigung zum Anzeigen von Details zu Preisplänen	Lesen			
ListPricingPlansAssociatedWithPricingRule	Gewährt die Berechtigung zum Auflisten von Preisplänen, die mit einer Preisregel verknüpft sind	Auflisten	pricingrule*		
ListPricingRules	Gewährt die Berechtigung zum Anzeigen von Details zu Preisregeln	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListPricingRulesAssociatedToPricingPlan	Gewährt die Berechtigung zum Auflisten von Preisregeln, die mit einem Preisplan verknüpft sind	Auflisten	pricingplan*		
ListResourcesAssociatedToCustomLineItem	Gewährt die Berechtigung, Ressourcen aufzulisten, die mit einem benutzerdefinierten Prozent-Einzelposten verknüpft sind	Auflisten	customlineitem*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags einer Ressource	Lesen	billinggroup		
			customlineitem		
			pricingplan		
			pricingrule		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren	billinggroup		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			customlineitem		
			pricingplan		
			pricingrule		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Markierung	billinggroup		
			customlineitem		
			pricingplan		
			pricingrule		
				aws:TagKeys	
UpdateBillingGroup	Gewährt die Berechtigung zum Aktualisieren einer Fakturierungsgruppe	Schreiben	billinggroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateCustomLineItem	Gewährt die Berechtigung zum Aktualisieren eines benutzerdefinierten Einzelpostens	Schreiben	customlineitem*		
UpdatePricingPlan	Gewährt die Berechtigung zum Aktualisieren eines Preisplans	Schreiben	pricingplan*		
UpdatePricingRule	Gewährt die Berechtigung zum Aktualisieren einer Preisregel	Schreiben	pricingrule*		

Von AWS Billing Conductor definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
billinggroup	`arn:${Partition}:billingconductor::${Account}:billinggroup/${BillingGroupId}`	aws:ResourceTag/${TagKey}
pricingplan	`arn:${Partition}:billingconductor::${Account}:pricingplan/${PricingPlanId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
pricingrule	`arn:${Partition}:billingconductor::${Account}:pricingrule/${PricingRuleId}`	aws:ResourceTag/${TagKey}
customlineitem	`arn:${Partition}:billingconductor::${Account}:customlineitem/${CustomLineItemId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Billing Conductor

AWS Billing Conductor definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Billing-Konsole

AWS Billing-Konsole (Servicepräfix: `aws-portal`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von der AWS Billing-Konsole definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetConsoleActionSetEnforced [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen, ob vorhandene oder detaillierte IAM-Aktionen verwendet werden, um die Autorisierung für die Fakturierungs-, Kostenmanagement- und Kontokonsolen zu steuern	Lesen			
ModifyAccount [nur Berechtigung]	IAM-Benutzer die Berechtigung zum Ändern von Kontoeinstellungen erteilen oder verweigern	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyBilling [nur Berechtigung]	IAM-Benutzern die Berechtigung zum Ändern von Abrechnungseinstellungen gewähren oder verweigern	Schreiben			
ModifyPaymentMethods [nur Berechtigung]	IAM-Benutzern die Berechtigung zum Ändern von Zahlungsmethoden gewähren oder verweigern	Schreiben			
UpdateConsoleActionSetEnforced [nur Berechtigung]	Gewährt die Berechtigung zum Ändern, ob vorhandene oder detaillierte IAM-Aktionen verwendet werden sollen, um die Autorisierung für die Fakturierungs-, Kostenmanagement- und Kontokonsolen zu steuern	Schreiben			
ViewAccount [nur Berechtigung]	IAM-Benutzern die Berechtigung zum Anzeigen von Kontoeinstellungen gewähren oder verweigern	Lesen			
ViewBilling [nur Berechtigung]	IAM-Benutzern die Berechtigung zum Anzeigen von Fakturierungsseiten in der Konsole gewähren oder verweigern	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ViewPaymentMethods [nur Berechtigung]	IAM-Benutzern die Berechtigung zum Anzeigen von Zahlungsmethoden gewähren oder verweigern	Lesen			
ViewUsage [nur Berechtigung]	IAM-Benutzern die Berechtigung zum Anzeigen von AWS-Nutzungsberichten gewähren oder verweigern	Lesen			

Von der AWS Billing-Konsole definierte Ressourcentypen

Die AWS Billing-Konsole unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf die AWS Billing-Konsole zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Billing-Konsole

Die Abrechnungskonsole besitzt keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Braket

Amazon Braket (Servicepräfix: `braket`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.

- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Braket definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptUserAgreement	Gewährt die Berechtigung zum Akzeptieren der Amazon Braket-Benutzervereinbarung	Schreiben			
AccessBraketFeature	Gewährt die Berechtigung zum Überprüfen, ob ein Amazon-Braket-Feature für ein Konto aktiviert ist. Kunden benötigen diese Berechtigung, um alle in der Konsole verfügbaren Features nutzen zu können	Lesen			
CancelJob	Gewährt die Berechtigung zum Abbrechen einer Aufgabe.	Schreiben	job*		
CancelQuantumTask	Gewährt die Berechtigung zum Abbrechen einer Quantenaufgabe	Schreiben	quantum-task*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateJob	Gewährt die Berechtigung zum Erstellen eines Auftrags.	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateQuantumTask	Gewährt die Berechtigung zum Erstellen einer Quantenaufgabe	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
GetDevice	Gewährt die Berechtigung zum Abrufen von Informationen über die in Amazon Braket verfügbaren Geräte	Lesen			
GetJob	Gewährt die Berechtigung zum Abrufen von Aufträgen	Lesen	job*		
GetQuantumTask	Gewährt die Berechtigung zum Abrufen von Quantenaufgaben	Lesen	quantum-task*		
GetServiceLinkedRoleStatus	Gewährt die Berechtigung zum Überprüfen, ob die mit dem Amazon-Braket-Service verknüpfte Rolle erstellt wurde.	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetUserAgreementStatus	Gewährt die Berechtigung zum Überprüfen, ob das Konto die Amazon-Braket-Benutzervereinbarung akzeptiert hat.	Lesen			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags, die auf die Quantenaufgaben-Ressource oder den Auftrag angewendet wurden	Lesen	job quantum-task		
SearchDevices	Gewährt die Berechtigung zum Suchen nach Geräten, die in Amazon Braket verfügbar sind	Lesen			
SearchJobs	Gewährt die Berechtigung zum Suchen nach Aufträgen	Lesen			
SearchQuantumTasks	Gewährt die Berechtigung zum Suchen nach Quantenaufgaben	Lesen			
TagResource	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Tags zu einer Quantenaufgabe oder einem hybriden Auftrag	Markierung	job quantum-task		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung, ein oder mehrere Tags aus einer Quantenaufgabenressource oder einem Auftrag zu entfernen. Ein Tag besteht aus einem Schlüssel-Wert-Paar	Markieren	job		
			quantum-task		
				aws:TagKeys	

Von Amazon Braket definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
quantum-task	`arn:${Partition}:braket:${Region}:${Account}:quantum-task/${RandomId}`	aws:ResourceTag/${TagKey}
job	`arn:${Partition}:braket:${Region}:${Account}:job/${JobName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Braket

Amazon Braket definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Budget Service

AWS Budget Service (Dienstpräfix:`budgets`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Budget Service definierte Aktionen

- Von AWS Budget Service definierte Ressourcentypen
- Bedingungsschlüssel für AWS Budget Service

Von AWS Budget Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

> **Note**
>
> Bei den Aktionen in dieser Tabelle handelt es sich nicht um APIs, sondern um Berechtigungen, die Zugriff auf die AWS Billing and Cost Management APIs gewähren, die auf Budgets zugreifen.

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateBudgetAction	Erteilt die Berechtigung, eine Antwort zu konfigurieren, die ausgeführt wird, sobald Ihr Budget einen bestimmten Budgetschwellenwert überschreitet. Für das Erstellen einer Budgetaktion mit Tags ist außerdem die Berechtigung „Budgets: TagResource“ erforderlich	Schreiben	budgetAction*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteBudgetAction	Gewährt die Berechtigung zum Löschen einer Aktion, die einem bestimmten Budget zugeordnet ist	Schreiben	budgetAction*		
DescribeBudgetAction	Gewährt die Berechtigung zum Abrufen der Details einer bestimmten Budgetaktion, die mit einem Budget verknüpft ist	Lesen	budgetAction*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeBudgetActionHistories	Gewährt die Berechtigung zum Abrufen einer historischen Ansicht der Status von Budgetvorgängen, die einer bestimmten Budgetaktion zugeordnet sind. Dazu zählen Status wie „Standby“, „Ausstehend“ und „Ausgeführt“	Lesen	budgetAction*		
DescribeBudgetActionsForAccount	Gewährt die Berechtigung zum Abrufen der Details aller Budgetaktionen, die mit Ihrem Konto verknüpft sind	Lesen			
DescribeBudgetActionsForBudget	Gewährt die Berechtigung zum Abrufen der Details aller Budgetaktionen, die mit einem Budget verknüpft sind	Lesen	budget*		
ExecuteBudgetAction	Gewährt die Berechtigung zum Starten einer ausstehenden Budgetaktion sowie zur Umkehrung einer zuvor ausgeführten Budgetaktion	Schreiben	budgetAction*		
ListTagsForResource	Erteilt die Berechtigung zum Anzeigen von Ressourcen-Tags für ein Budget oder eine Budgetaktion	Lesen	budget budgetAction		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyBudget	Erteilt die Berechtigung zum Erstellen und Ändern von Budgets sowie zum Bearbeiten von Budgetdetails. Für die Erstellung eines Budgets mit Stichwörtern ist außerdem die Berechtigung „Budgets: TagResource“ erforderlich	Schreiben	budget*		
TagResource	Erteilt die Berechtigung, Ressourcen-Tags auf ein Budget oder eine Budgetaktion anzuwenden. Wird auch benötigt, um ein Budget oder eine Budgetaktion mit Tags zu erstellen	Tagging	budget		
			budgetAction		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Erteilt die Berechtigung, Ressourcen-Tags aus einem Budget oder einer Budgetaktion zu entfernen	Tagging	budget		
			budgetAction		
				aws:TagKeys	
UpdateBudgetAction	Gewährt die Berechtigung zum Aktualisieren der Details einer bestimmten Budgetaktion, die einem Budget zugeordnet ist	Schreiben	budgetAction*		iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ViewBudget	Gewährt die Berechtigung zum Anzeigen von Budgets und von Budgetdetails	Lesen	budget*		

Von AWS Budget Service definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
budget	`arn:${Partition}:budgets::${Account}:budget/${BudgetName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
budgetAction	`arn:${Partition}:budgets::${Account}:budget/${BudgetName}/action/${ActionId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Bedingungsschlüssel für AWS Budget Service

AWS Budget Service definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüsseln, die in der Anforderung übergeben werden.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS BugBust

AWS BugBust (Servicepräfix: `bugbust`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS BugBust definierte Aktionen

- Von BugBust AWS definierte Ressourcentypen
- Bedingungsschlüssel für AWS BugBust

Von AWS BugBust definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateEvent [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines BugBust-Ereignisses	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
EvaluateProfilingGroups [nur Berechtigung]	Gewährt die Berechtigung zum Auswerten eingecheckter Profilerstellungsgruppen	Write	Event*		
				aws:ResourceTag/${TagKey}	
GetEvent [nur Berechtigung]	Gewährt Berechtigungen zum Anzeigen von Kundendetails zu einem Ereignis	Read	Event*		
				aws:ResourceTag/${TagKey}	
GetJoinEventStatus [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen des Status des Versuchs eines BugBust	Read	Event*		
				aws:ResourceTag/${TagKey}	
JoinEvent [nur Berechtigung]	Gewährt die Berechtigung zum Mitmachen einer Veranstaltung	Write	Event*		
				aws:ResourceTag/${TagKey}	
ListBugs [nur Berechtigung]	Gewährt die Berechtigung, die Fehler anzuzeigen, die in ein	Read	Event*		codeguru-reviewer:

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Ereignis importiert wurden, um damit zu arbeiten				DescribeCodeReview codeguru-reviewer:ListRecommendations
				aws:ResourceTag/${TagKey}	
ListEventParticipants [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen der Teilnehmer einer Veranstaltung	Read	Event*		
				aws:ResourceTag/${TagKey}	
ListEventScores [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen der Punktzahl der Spieler	Read	Event*		
				aws:ResourceTag/${TagKey}	
ListEvents [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von BugBust	List		aws:ResourceTag/${TagKey}	
ListProfilingGroups [nur Berechtigung]	Gewährt die Berechtigung, die Profilinggruppen anzuzeigen, die in ein Ereignis importiert wurden, um damit zu arbeiten	Read	Event*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListPullRequests [nur Berechtigung]	Gewährt die Berechtigung, die Pull-Anfragen anzuzeigen, die von Spielern verwendet werden, um Korrekturen für ihre beanspruchten Fehler in einem Ereignis einzureichen	Read	Event*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Tags für eine Bugbust-Ressource	Read	Event*		
				aws:ResourceTag/${TagKey}	
TagResource [nur Berechtigung]	Gewährt die Berechtigung zum Markieren einer Bugbust-Ressource	Markieren	Event*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [nur Berechtigung]	Gewährt die Berechtigung zum Aufheben der Markierung einer Bugbust-Ressource	Markieren	Event*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateEvent [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren eines BugBust-Ereignisses	Write	Event*		codeguru-profiler:DescribeProfilingGroup codeguru-profiler:ListProfilingGroups codeguru-reviewer:DescribeCodeReview codeguru-reviewer:ListCodeReviews codeguru-reviewer:ListRecommendations codeguru-reviewer:TagResource

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					codeguru-reviewer:UnTagResource
				aws:ResourceTag/${TagKey}	
UpdateWorkItem [nur Berechtigung]	Gewährt die Berechtigung, ein Arbeitselement als beansprucht oder nicht beansprucht zu aktualisieren (Fehler oder Profilerstellungsgruppe)	Write	Event*		codeguru-reviewer:ListRecommendations
				aws:ResourceTag/${TagKey}	
UpdateWorkItemAdmin [nur Berechtigung]	Gewährt die Berechtigung, das Arbeitselement eines Ereignisses zu aktualisieren (Fehler oder Profilerstellungsgruppe)	Write	Event*		codeguru-reviewer:ListRecommendations
				aws:ResourceTag/${TagKey}	

Von BugBust AWS definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der

Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Event	`arn:${Partition}:bugbust:${Region}:${Account}:events/${EventId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS BugBust

AWS BugBust definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüsseln, die in der Anforderung übergeben werden.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Certificate Manager

AWS Certificate Manager (Servicepräfix: `acm`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Certificate Manager definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddTagsToCertificate	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Tags zu einem Zertifikat	Markieren	certificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCertificate	Gewährt die Berechtigung zum Löschen eines Zertifikats und des zugehörigen privaten Schlüssels	Write	certificate*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeCertificate	Gewährt die Berechtigung zum Abrufen von Zertifikaten und ihren Metadaten	Read	certificate*		
ExportCertificate	Gewährt die Berechtigung zum Exportieren eines privaten Zertifikats, das von einer Private Certificate Authority ausgegeben wurde	Read	certificate*		
GetAccountConfiguration	Gewährt die Berechtigung zum Abrufen der Konfiguration auf Kontoebene von AWS Certificate Manager	Lesen			
GetCertificate	Gewährt die Berechtigung zum Abrufen eines Zertifikats und der Zertifikatskette für einen Zertifikat-ARN	Lesen	certificate*		
ImportCertificate	Gewährt die Berechtigung zum Importieren eines Zertifikats von Drittanbietern in AWS Certificate Manager (ACM)	Schreiben	certificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListCertificates	Gewährt die Berechtigung zum Abrufen einer Liste der Zertifikat-ARNs und der Domain-Namen für jeden ARN	List			
ListTagsForCertificate	Gewährt die Berechtigung zum Auflisten der Tags, die einem Zertifikat zugeordnet wurden	Read	certificate*		
PutAccountConfiguration	Gewährt die Berechtigung zum Aktualisieren der Konfiguration auf Kontoebene in AWS Certificate Manager	Write			
RemoveTagsFromCertificate	Gewährt die Berechtigung zum Entfernen eines oder mehrerer Tags aus einem Zertifikat	Markieren	certificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RenewCertificate	Gewährt die Berechtigung zum Erneuern eines zulässigen privaten Zertifikats	Write	certificate*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RequestCertificate	Gewährt die Berechtigung zum Anfordern eines öffentlichen oder privaten Zertifikats	Write		aws:RequestTag/${TagKey} aws:TagKeys acm:DomainNames acm:CertificateTransparencyLogging acm:ValidationMethod acm:KeyAlgorithm acm:CertificateAuthority	
ResendValidationEmail	Gewährt die Berechtigung zum erneuten Senden einer E-Mail, um eine Validierung der Domain-Eigentümerschaft anzufordern	Write	certificate*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateCertificateOptions	Gewährt die Berechtigung zum Aktualisieren der Konfiguration eines Zertifikats Wird verwendet, um anzugeben, ob eine An- oder Abmeldung für die Protokollierung der Zertifikatstransparenz erfolgt	Schreiben	certificate*		

Von AWS Certificate Manager definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
certificate	`arn:${Partition}:acm:${Region}:${Account}:certificate/${CertificateId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Certificate Manager

AWS Certificate Manager definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
acm:CertificateAuthority	Filtert den Zugriff anhand der Option CertificateAuthority in der Anfrage. Kann verwendet werden, um einzuschränken, von welchen Zertifizierungsstellen Zertifikate ausgestellt werden können	Zeichenfolge
acm:CertificateTransparencyLogging	Filtert den Zugriff anhand der Option certificateTransparencyLogging in der Anfrage. Der Standardwert lautet „ENABLED“, wenn in der Anfrage kein Schlüssel vorhanden ist	Zeichenfolge
acm:DomainNames	Filtert den Zugriff anhand der Option domainNames in der Anfrage. Dieser Schlüssel kann verwendet werden, um einzuschränken, welche Domains in Zertifikatsanfragen enthalten sein dürfen	ArrayOfString
acm:KeyAlgorithm	Filtert den Zugriff anhand der Option keyAlgorithmus in der Anfrage	Zeichenfolge
acm:ValidationMethod	Filtert den Zugriff anhand der Option validationMethod in der Anfrage. Der Standartwert lautet „EMAIL“, wenn in der Anfrage kein Schlüssel vorhanden ist	Zeichenfolge
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Chatbot

AWS Chatbot (Servicepräfix: `chatbot`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Chatbot definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateChimeWebhookConfiguration	Gewährt die Berechtigung zum Erstellen einesAWSChatbot Chime Webhook-Konfiguration	Schreiben			
CreateMicrosoftTeamsChannelConfiguration	Gewährt die Berechtigung zum Erstellen einer Kanalkonfiguration von AWS Chatbot Microsoft Teams	Schreiben			
CreateSlackChannelConfiguration	Gewährt die Berechtigung zum Erstellen einesAWSChatbot Slack-Channel-Konfiguration	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteChimeWebhookConfiguration	Gewährt die Berechtigung zum Löschen einesAWSChatbot Chime Webhook-Konfiguration	Schreiben	ChatbotConfiguration*		
DeleteMicrosoftTeamsChannelConfiguration	Gewährt die Berechtigung zum Löschen einer Kanalkonfiguration von AWS Chatbot Microsoft Teams	Schreiben			
DeleteMicrosoftTeamsConfiguredTeam	Gewährt die Berechtigung zum Löschen der mit AWS Chatbot in einem AWS-Konto konfigurierten Microsoft Teams	Schreiben			
DeleteMicrosoftTeamsUserIdentity	Gewährt die Berechtigung zum Löschen einer Benutzeridentität von AWS Chatbot Microsoft Teams	Schreiben			
DeleteSlackChannelConfiguration	Gewährt die Berechtigung zum Löschen einesAWSChatbot Slack-Channel-Konfiguration	Schreiben	ChatbotConfiguration*		
DeleteSlackUserIdentity	Gewährt die Berechtigung zum Löschen einer AWS-Chatbot-Slack-Benutzeridentität	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteSlackWorkspaceAuthorization	Gewährt die Berechtigung zum Löschen der Slack Workspace Berechtigung mitAWSChatbot, der mit einemAWS-Konto	Schreiben			
DescribeChimeWebhookConfigurations	Gewährt die Berechtigung, alle AWS-Chatbot-Chime-Webhook-Konfigurationen in einem AWS-Konto aufzulisten	Lesen			
DescribeSlackChannelConfigurations	Gewährt die Berechtigung zum Auflisten allerAWSChatbot Slack-Channel-Konfigurationen in einemAWS-Konto	Lesen			
DescribeSlackChannels	Gewährt die Berechtigung, alle öffentlichen Slack-Kanäle im Slack-Workspace aufzulisten, die mit dem in den AWS-Chatbot-Service integrierten AWS-Konto verbunden sind	Lesen			
DescribeSlackUserIdentities	Gewährt die Berechtigung zum Beschreiben von AWS-Chatbot-Slack-Benutzeridentitäten	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeSlackWorkspaces	Gewährt die Berechtigung, alle autorisierten Slack-Workspaces aufzulisten, die mit dem in den AWS-Chatbot-Service integrierten AWS-Konto verbunden sind	Lesen			
GetAccountPreferences	Gewährt die Berechtigung zum Abrufen der Kontoeinstellungen für AWS Chatbot	Lesen			
GetMicrosoftTeamsChannelConfiguration	Gewährt die Berechtigung zum Abrufen einer einzelnen Kanalkonfiguration von AWS Chatbot Microsoft Teams in einem AWS-Konto	Lesen			
GetMicrosoftTeamsOauthParameters	Gewährt die Berechtigung zum Generieren von OAuth-Parameter, um den OAuth-Code für Microsoft Teams anzufordern, der vom AWS-Chatbot-Service verwendet werden soll	Lesen			
GetSlackOauthParameters	Gewährt die Berechtigung zum Generieren von OAuth-Parameter, um den Slack-OAuth-Code anzufordern, der vom AWS-Chatbot-Service verwendet werden soll	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListMicrosoftTeamsChannelConfigurations	Gewährt die Berechtigung zum Auflisten aller Kanalkonfigurationen von AWS Chatbot Microsoft Teams in einem AWS-Konto	Lesen			
ListMicrosoftTeamsConfiguredTeams	Gewährt die Berechtigung zum Auflisten aller Microsoft Teams, die mit dem in den AWS-Chatbot-Service integrierten AWS-Konto verbunden sind	Lesen			
ListMicrosoftTeamsUserIdentities	Gewährt die Berechtigung zum Beschreiben von Benutzeridentitäten von AWS Chatbot Microsoft Teams	Lesen			
RedeemMicrosoftTeamsOauthCode	Gewährt die Berechtigung zum Einlösen zuvor generierter Parameter mit Microsoft-Teams-APIs, um OAuth-Token zu erwerben, die vom AWS-Chatbot-Service verwendet werden sollen	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RedeemSlackOauthCode	Gewährt die Berechtigung zum Einlösen zuvor generierter Parameter mit der Slack-API, um OAuth-Token zu erwerben, die vom AWS-Chatbot-Service verwendet werden sollen	Schreiben			
UpdateAccountPreferences	Gewährt die Berechtigung zum Aktualisieren der Kontoeinstellungen für AWS Chatbot	Schreiben			
UpdateChimeWebhookConfiguration	Gewährt die Berechtigung zum Aktualisieren einesAWSChatbot Chime Webhook-Konfiguration	Schreiben	ChatbotConfiguration*		
UpdateMicrosoftTeamsChannelConfiguration	Gewährt die Berechtigung zum Aktualisieren einer Kanalkonfiguration von AWS Chatbot Microsoft Teams	Schreiben			
UpdateSlackChannelConfiguration	Gewährt die Berechtigung zum Aktualisieren der Konfiguration eines AWS-Chatbot-Slack-Kanals	Schreiben	ChatbotConfiguration*		

Von AWS Chatbot definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der

Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
ChatbotConfiguration	`arn:${Partition}:chatbot::${Account}:chat-configuration/${ConfigurationType}/${ChatbotConfigurationName}`	

Bedingungsschlüssel für AWS Chatbot

Chatbot besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Chime

Amazon Chime (Servicepräfix: `chime`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Chime definierte Aktionen
- Von Amazon Chime definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Chime

Von Amazon Chime definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptDelegate	Gewährt die Berechtigung zum Annehmen der Delegierungseinladung für die gemeinsame Verwaltung eines Amazon-Chime-Kontos mit einem anderen AWS-Konto.	Write			
ActivateUsers	Gewährt die Berechtigung zum Aktivieren von Benutzern in einem Amazon Chime Enterprise-Konto.	Write			
AddDomain	Gewährt die Berechtigung Ihrem Amazon-Chime-Konto eine Domain hinzuzufügen	Write			
AddOrUpdateGroups	Gewährt die Berechtigung zum Hinzufügen neuer oder zum Aktualisieren vorhandener Active Directory- oder Okta-Benutzergruppen, die dem Amazon Chime Enterprise-Konto zugeordnet sind.	Schreiben			
AssociateChannelFlow	Gewährt die Berechtigung, einen Flow mit einem Kanal zu verknüpfen	Schreiben	app-instance-bot*		
			app-instance-user*		
			channel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			channel-flow*		
AssociatePhoneNumberWithUser	Gewährt die Berechtigung, eine Telefonnummer mit einem Amazon-Chime-Benutzer zu verknüpfen.	Write			
AssociatePhoneNumbersWithVoiceConnector	Gewährt die Berechtigung zum Verknüpfen mehrerer Telefonnummern mit einem Amazon Chime Voice Connector.	Write	voice-connector*		
AssociatePhoneNumbersWithVoiceConnectorGroup	Gewährt die Berechtigung zum Verknüpfen mehrerer Telefonnummern mit einer Amazon Chime Voice Connector-Gruppe.	Schreiben			
AssociateSigninDelegateGroupsWithAccount	Gewährt die Berechtigung, die angegebenen Anmeldedelegatgruppen dem angegebenen Amazon-Chime-Konto zuzuordnen.	Schreiben			
AuthorizeDirectory	Gewährt die Berechtigung zum Autorisieren eines Active Directory für das Amazon Chime Enterprise-Konto.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchCreateAttendee	Gewährt die Berechtigung zum Erstellen neuer Teilnehmer für ein aktives Amazon Chime SDK-Meeting.	Schreiben	meeting*		
BatchCreateChannelMembership	Gewährt die Berechtigung zum Hinzufügen mehrerer Benutzer und Bots zu einem Kanal	Schreiben	app-instance-bot*		
			app-instance-user*		
			channel*		
BatchCreateRoomMembership	Gewährt die Berechtigung zum stapelweisen Hinzufügen von Raummitgliedern.	Write			
BatchDeletePhoneNumber	Gewährt die Berechtigung zum Verschieben von bis zu 50 Telefonnummern in die Löschwarteschlange.	Write			
BatchSuspendUser	Gewährt die Berechtigung zum Aussetzen von bis zu 50 Benutzern eines Team- oder EnterpriseLWA Amazon-Chime-Kontos.	Write			
BatchUnsuspendUser	Gewährt die Berechtigung zum Aufheben der Aussetzung von bis zu 50 Benutzern für das angegebene Amazon Chime EnterpriseLWA-Konto.	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchUpdateAttendeeCapabilitiesExcept	Gewährt die Berechtigung zum Aktualisieren von AttendeeCapabilities mit Ausnahme der in einer ExcludedAttendeeIDs-Tabelle aufgeführten Funktionen.	Schreiben	meeting*		
BatchUpdatePhoneNumber	Gewährt die Berechtigung zum Aktualisieren von Telefonnummerndetails im UpdatePhoneNumberRequestItem-Objekt für bis zu 50 Telefonnummern.	Write			
BatchUpdateUser	Gewährt die Berechtigung zum Aktualisieren der Benutzerdaten im UpdateUserRequestItem-Objekt für bis zu 20 Benutzer für das angegebene Amazon-Chime-Konto.	Schreiben			
ChannelFlowCallback	Gewährt die Berechtigung zum Rückruf für eine Nachricht in einem Kanal	Schreiben	channel*		
Connect	Gewährt die Berechtigung zum Herstellen einer Websocket-Verbindung für App-Instance-Benutzer zum Endpunkt der Messaging-Sitzung	Write	app-instance-user*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ConnectDirectory	Gewährt die Berechtigung zum Verbinden eines Active Directory mit dem Amazon Chime Enterprise-Konto.	Write			ds:ConnectDirectory
CreateAccount	Gewährt die Berechtigung zum Erstellen eines Amazon-Chime-Kontos unter dem AWS-Konto des Administrators.	Write			
CreateApiKey	Gewährt die Berechtigung zum Erstellen eines neuen SCIM-Zugriffsschlüssels für das Amazon-Chime-Konto und die Okta-Konfiguration.	Write			
CreateAppInstance	Gewährt die Berechtigung zum Erstellen einer App-Instance unter dem AWS-Konto.	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAppInstanceAdmin	Gewährt die Berechtigung zum Befördern eines Benutzers oder Bots zu einem AppInstanceAdmin	Schreiben	app-instance*		
			app-instance-bot*		
			app-instance-user*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAppInstanceBot	Gewährt die Berechtigung zum Erstellen eines Bots unter einer Amazon-Chime-AppInstance	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAppInstanceUser	Gewährt die Berechtigung zum Erstellen eines Benutzers unter einer Amazon-Chime-AppInstance	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAttendee	Gewährt die Berechtigung zum Erstellen eines neuen Teilnehmers für ein aktives Amazon Chime SDK-Meeting.	Write	meeting*		
CreateBot	Gewährt die Berechtigung zum Erstellen eines Bots für ein Amazon Chime Enterprise Konto.	Schreiben			
CreateCDRBucket	Gewährt die Berechtigung zum Erstellen eines neuen S3 Buckets für Anrufdetailakten.	Write			s3:CreateBucket s3:ListAllMyBuckets

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateChannel	Gewährt die Berechtigung zum Erstellen eines Kanals für eine App-Instance unter dem AWS-Konto.	Schreiben	app-instance-bot*		
			app-instance-user*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateChannelBan	Gewährt die Berechtigung zum Sperren eines Benutzers für einen Kanal	Schreiben	app-instance-bot*		
			app-instance-user*		
			channel*		
CreateChannelFlow	Gewährt die Berechtigung zum Erstellen eines Kanal-Flows für eine App-Instance unter dem AWS-Konto	Schreiben	app-instance*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateChannelMembership	Gewährt die Berechtigung zum Hinzufügen eines Benutzers oder Bots zu einem Kanal	Schreiben	app-instance-bot*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			app-instance-user*		
			channel*		
CreateChannelModerator	Gewährt die Berechtigung zum Erstellen eines Kanalmoderators	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
CreateMediaCapturePipeline	Gewährt die Berechtigung zum Erstellen einer Pipeline zur Medienerfassung.	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	s3:GetBucketPolicy
CreateMediaConcatenationPipeline	Gewährt die Berechtigung zum Erstellen einer Pipeline zur Medienverkettung	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	s3:GetBucketPolicy
CreateMediaInsightsPipeline	Gewährt die Berechtigung zum Erstellen einer Pipeline zu Medienerkenntnissen	Schreiben	media-insights-pipeline-configuration*		chime:TagResource kinesisvideo:DescribeStream

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateMediaInsightsPipelineConfiguration	Gewährt die Berechtigung zum Erstellen einer Pipelinekonfiguration zu Medienerkenntnissen	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	chime:TagResource iam:PassRole kinesis:DescribeStream s3:ListBucket
CreateMediaLiveConnectorPipeline	Gewährt die Berechtigung zum Erstellen einer Media-Live-Connector-Pipeline	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateMediaPipelineKinesisVideoStreamPool	Gewährt die Berechtigung zum Erstellen eines Kinesis-Videostreampools	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	kinesis:DescribeStream kinesisvideo:CreateStream kinesisvideo:GetDataEndpoint kinesisvideo:ListStreams
CreateMediaStreamPipeline	Gewährt die Berechtigung zum Erstellen einer Medienstreampipeline	Schreiben	media-pipeline-kinesis-video-stream-pool*		kinesisvideo:DescribeStream kinesisvideo:GetDataEndpoint kinesisvideo:PutMedia

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateMeeting	Gewährt die Berechtigung zum Erstellen eines neuen Amazon-Chime-SDK-Meetings in der angegebenen Medienregion ohne anfängliche Teilnehmer.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMeetingDialOut	Gewährt die Berechtigung, eine Telefonnummer anzurufen, um am angegebenen Amazon-Chime-SDK-Meeting teilzunehmen	Write	meeting*		
CreateMeetingWithAttendees	Gewährt die Berechtigung zum Erstellen eines neuen Amazon-Chime-SDK-Meetings in der angegebenen Medienregion mit einer Gruppe von Teilnehmern	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePhoneNumberOrder	Gewährt die Berechtigung zum Erstellen einer Telefonnummernbeantragung bei Netzbetreibern.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateProxySession	Gewährt die Berechtigung zum Erstellen einer Proxysitzung für den angegebenen Amazon Chime Voice Connector.	Write	voice-connector*		
CreateRoom	Gewährt die Berechtigung zum Erstellen eines Raums.	Write			
CreateRoomMembership	Gewährt die Berechtigung zum Hinzufügen eines Raummitglieds.	Write			
CreateSipMediaApplication	Gewährt die Berechtigung zum Erstellen einer Amazon-Chime-SIP-Medienanwendung unter dem AWS-Konto des Administrators.	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateSipMediaApplicationCall	Gewährt die Berechtigung zum Erstellen eines ausgehenden Anrufs für die Amazon-Chime-SIP-Medienanwendung unter dem AWS-Konto des Administrators.	Write	sip-media-application*		
CreateSipRule	Gewährt die Berechtigung zum Erstellen einer Amazon-Chime-SIP-Regel unter dem AWS-Konto des Administrators.	Schreiben	sip-media-application		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateUser	Gewährt die Berechtigung zum Erstellen eines Benutzers unter dem angegebenen Amazon-Chime-Konto.	Schreiben			
CreateVoiceConnector	Gewährt die Berechtigung zum Erstellen eines Amazon Chime Voice Connectors im AWS-Konto des Administrators.	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateVoiceConnectorGroup	Gewährt die Berechtigung zum Erstellen einer Amazon Chime Voice Connector-Gruppe im AWS-Konto des Administrators.	Schreiben	voice-connector		
CreateVoiceProfile	Gewährt die Berechtigung zum Erstellen eines Sprachprofils	Schreiben			
CreateVoiceProfileDomain	Gewährt die Berechtigung zum Erstellen einer Sprachprofil-Domain	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	chime:TagResource kms:CreateGrant kms:DescribeKey
DeleteAccount	Gewährt die Berechtigung zum Löschen der angegebenen Amazon-Chime-Kontos.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteAccountOpenIdConfig	Gewährt die Berechtigung zum Löschen der OpenIdConfig-Attribute aus Ihrem Amazon-Chime-Konto.	Write			
DeleteApiKey	Gewährt die Berechtigung zum Löschen des angegebenen SCIM-Zugriffsschlüssels, der dem Amazon-Chime-Konto und der Okta-Konfiguration zugeordnet ist.	Write			
DeleteAppInstance	Gewährt die Berechtigung zum Löschen einer AppInstance	Schreiben	app-instance*		
DeleteAppInstanceAdmin	Gewährt die Berechtigung zum Befördern eines AppInstanceAdmin zu einem Benutzer oder Bot	Schreiben	app-instance*		
			app-instance-bot*		
			app-instance-user*		
DeleteAppInstanceBot	Gewährt die Berechtigung zum Löschen eines AppInstanceBot	Schreiben	app-instance-bot*		
DeleteAppInstanceStreamingConfigurations	Gewährt die Berechtigung, Datenstreaming für die App-Instance zu deaktivieren	Write	app-instance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteAppInstanceUser	Gewährt die Berechtigung zum Löschen eines AppInstanceUser	Write	app-instance-user*		
DeleteAttendee	Gewährt die Berechtigung zum Löschen des angegebenen Teilnehmers aus einem Amazon Chime SDK-Meeting.	Write	meeting*		
DeleteCDRBucket	Gewährt die Berechtigung zum Löschen eines S3 Buckets für Anrufdetailakten aus Ihrem Amazon-Chime-Konto.	Write			s3:DeleteBucket
DeleteChannel	Gewährt die Berechtigung zum Löschen eines Channels.	Schreiben	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteChannelBan	Gewährt die Berechtigung zum Entfernen eines Benutzers oder Bots aus der Sperrliste eines Kanals	Schreiben	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteChannelFlow	Gewährt die Berechtigung zum Löschen eines Kanal-Flows	Schreiben	channel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteChannelMembership	Gewährt die Berechtigung, ein Mitglied aus einem Kanal zu entfernen	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteChannelMessage	Gewährt die Berechtigung zum Löschen einer Nachricht in einem Kanal	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteChannelModerator	Gewährt die Berechtigung zum Löschen eines Kanalmoderators	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteDelegate	Gewährt die Berechtigung zum Löschen des delegierten AWS-Konto-Managements aus dem Amazon-Chime-Konto.	Write			
DeleteDomain	Gewährt die Berechtigung zum Löschen einer Domain aus dem Amazon-Chime-Konto	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteEventsConfiguration	Gewährt die Berechtigung zum Löschen einer Event-Konfiguration, sodass ein Bot ausgehende Ereignisse empfangen kann.	Write			
DeleteGroups	Gewährt die Berechtigung zum Löschen von Active Directory- oder Okta-Benutzergruppen aus dem Amazon Chime Enterprise-Konto.	Write			
DeleteMediaCapturePipeline	Gewährt die Berechtigung zum Löschen einer Pipeline zur Medienerfassung.	Schreiben	media-pipeline*		
DeleteMediaInsightsPipelineConfiguration	Gewährt die Berechtigung zum Löschen einer Pipelinekonfiguration zu Medienerkenntnissen	Schreiben	media-insights-pipeline-configuration*		chime:ListVoiceConnectors
DeleteMediaPipeline	Gewährt die Berechtigung zum Löschen einer Medien-Pipeline	Schreiben	media-pipeline*		
DeleteMediaPipelineKinesisVideoStreamPool	Gewährt die Berechtigung zum Löschen eines Kinesis-Videostreampools	Schreiben	media-pipeline-kinesis-video-stream-pool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteMeeting	Gewährt die Berechtigung zum Löschen des angegebenen Amazon-Chime-SDK-Meetings.	Schreiben	meeting*		
DeleteMessagingStreamingConfigurations	Gewährt die Berechtigung zum Löschen von Datenstreaming-Konfigurationen einer AppInstance	Schreiben	app-instance*		
DeletePhoneNumber	Gewährt die Berechtigung, eine Telefonnummer in die Löschwarteschlange zu verschieben.	Write			
DeleteProxySession	Gewährt die Berechtigung zum Löschen einer Proxysitzung für den angegebenen Amazon Chime Voice Connector.	Write	voice-connector*		
DeleteRoom	Gewährt die Berechtigung zum Löschen eines Raums.	Write			
DeleteRoomMembership	Gewährt die Berechtigung zum Entfernen eines Raummitglieds.	Write			
DeleteSipMediaApplication	Gewährt die Berechtigung zum Löschen einer Amazon-Chime-SIP-Medienanwendung unter dem AWS-Konto des Administrators.	Write	sip-media-application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteSipRule	Gewährt die Berechtigung zum Löschen einer Amazon-Chime-SIP-Regel unter dem AWS-Konto des Administrators.	Write			
DeleteVoiceConnector	Gewährt die Berechtigung zum Löschen des angegebenen Amazon Chime Voice Connector.	Write	voice-connector*		logs:CreateLogDelivery logs:DeleteLogDelivery logs:GetLogDelivery logs:ListLogDeliveries
DeleteVoiceConnectorEmergencyCallingConfiguration	Gewährt die Berechtigung zum Löschen der Notrufkonfiguration für den angegebenen Amazon Chime Voice Connector.	Write	voice-connector*		
DeleteVoiceConnectorGroup	Gewährt die Berechtigung zum Löschen der angegebenen Amazon Chime Voice Connector-Gruppe.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteVoiceConnectorOrigination	Gewährt die Berechtigung zum Löschen der Ursprungseinstellungen für den angegebenen Amazon Chime Voice Connector.	Write	voice-connector*		
DeleteVoiceConnectorProxy	Gewährt die Berechtigung zum Löschen der Proxykonfiguration für den angegebenen Amazon Chime Voice Connector.	Write	voice-connector*		
DeleteVoiceConnectorStreamingConfiguration	Gewährt die Berechtigung zum Löschen der Streaming-Konfiguration für den angegebenen Amazon Chime Voice Connector.	Write	voice-connector*		
DeleteVoiceConnectorTermination	Gewährt die Berechtigung zum Löschen der Beendigungseinstellungen für den angegebenen Amazon Chime Voice Connector.	Write	voice-connector*		
DeleteVoiceConnectorTerminationCredentials	Gewährt die Berechtigung zum Löschen der SIP-Beendigungsanmeldeinformationen für den angegebenen Amazon Chime Voice Connector.	Schreiben	voice-connector*		
DeleteVoiceProfile	Gewährt die Berechtigung zum Löschen eines Sprachprofils	Schreiben	voice-profile*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteVoiceProfileDomain	Gewährt die Berechtigung zum Löschen einer Sprachprofil-Domain	Schreiben	voice-profile-domain*		
DeregisterAppInstanceUserEndpoint	Gewährt die Berechtigung zum Aufheben der Registrierung eines Endpunkts für einen App-Instance-Benutzer	Schreiben	app-instance-user*		
DescribeAppInstance	Gewährt die Berechtigung, alle Details zu einer AppInstance zu erhalten	Read	app-instance*		
DescribeAppInstanceAdmin	Gewährt die Berechtigung, alle Details zu einem AppInstanceAdmin zu erhalten	Lesen	app-instance*		
			app-instance-bot*		
			app-instance-user*		
DescribeAppInstanceBot	Gewährt die Berechtigung zum Abrufen der vollständigen Details eines AppInstanceBot	Lesen	app-instance-bot*		
DescribeAppInstanceUser	Gewährt die Berechtigung, alle Details zu einem AppInstanceUser zu erhalten	Lesen	app-instance-user*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeAppInstanceUserEndpoint	Gewährt die Berechtigung zum Beschreiben eines Endpunkts, der für einen App-Instance-Benutzer registriert ist	Lesen	app-instance-user*		
DescribeChannel	Gewährt die Berechtigung, alle Details zu einem Kanal zu erhalten	Read	app-instance-bot*		
			app-instance-user*		
			channel*		
DescribeChannelBan	Gewährt die Berechtigung, alle Details zu einer Kanalsperre zu erhalten	Lesen	app-instance-bot*		
			app-instance-user*		
			channel*		
DescribeChannelFlow	Gewährt die Berechtigung, alle Details zu einem Kanal-Flow zu erhalten	Lesen	channel-flow*		
DescribeChannelMembership	Gewährt die Berechtigung, alle Details zu einer Kanalmitgliedschaft zu erhalten	Lesen	app-instance-bot*		
			app-instance-user*		
			channel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeChannelMembershipForAppInstanceUser	Gewährt die Berechtigung zum Abrufen der Details zu einem Kanal anhand der Mitgliedschaft des angegebenen Benutzers oder Bots	Lesen	app-instance-bot*		
			app-instance-user*		
			channel*		
DescribeChannelModeratedByAppInstanceUser	Gewährt die Berechtigung zum Abrufen der vollständigen Details zu einem Kanal, der vom angegebenen Benutzer oder Bot moderiert wird	Lesen	app-instance-bot*		
			app-instance-user*		
			channel*		
DescribeChannelModerator	Gewährt die Berechtigung, alle Details zu einem ChannelModerator zu erhalten	Lesen	app-instance-bot*		
			app-instance-user*		
			channel*		
DisassociateChannelFlow	Gewährt die Berechtigung, einen Flow von einem Kanal zu trennen	Schreiben	app-instance-bot*		
			app-instance-user*		
			channel*		
			channel-flow*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociatePhoneNumberFromUser	Gewährt die Berechtigung zum Aufheben der Mapping der primär für den angegebenen Amazon-Chime-Benutzer bereitgestellten Telefonnummer.	Write			
DisassociatePhoneNumbersFromVoiceConnector	Gewährt die Berechtigung zum Aufheben der Mapping mehrerer Telefonnummern vom angegebenen Amazon Chime Voice Connector.	Write	voice-connector*		
DisassociatePhoneNumbersFromVoiceConnectorGroup	Gewährt die Berechtigung zum Aufheben der Mapping mehrerer Telefonnummern von der angegebenen Amazon Chime Voice Connector-Gruppe.	Schreiben			
DisassociateSigninDelegateGroupsFromAccount	Gewährt die Berechtigung, die Mapping der angegebenen Anmeldedelegatgruppen zum angegebenen Amazon-Chime-Konto aufzuheben.	Schreiben			
DisconnectDirectory	Gewährt die Berechtigung zum Trennen des Active Directory vom Amazon Chime Enterprise-Konto.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAccount	Gewährt die Berechtigung zum Abrufen von Details zum angegebenen Amazon-Chime-Konto.	Read			
GetAccountResource	Gewährt die Berechtigung zum Abrufen von Details der Konto Ressource, die dem Amazon-Chime-Konto zugeordnet ist.	Read			
GetAccountSettings	Gewährt die Berechtigung zum Abrufen von Kontoeinstellungen für die angegebene Amazon-Chime-Konto-ID.	Read			
GetAccountWithOpenIdConfig	Gewährt die Berechtigung zum Abrufen der Kontodetails und der OpenIdConfig-Attribute für Ihr Amazon-Chime-Konto.	Read			
GetAppInstanceRetentionSettings	Gewährt die Berechtigung zum Abrufen von Aufbewahrungseinstellungen für eine App-Instance	Read	app-instance*		
GetAppInstanceStreamingConfigurations	Gewährt die Berechtigung zum Abrufen der Streaming konfigurationen für eine App-Instance	Read	app-instance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAttendee	Gewährt die Berechtigung zum Abrufen von Teilnehmerdetails für eine angegebene Meeting-ID und Teilnehmer-ID.	Read	meeting*		
GetBot	Gewährt die Berechtigung zum Abrufen von Details für den angegebenen Bot.	Read			
GetCDRBucket	Gewährt die Berechtigung zum Abrufen der Details eines S3 Buckets für Anrufdetailakten, der dem Amazon-Chime-Konto zugeordnet ist.	Lesen			s3:GetBucketAcl s3:GetBucketLocation s3:GetBucketLogging s3:GetBucketVersioning s3:GetBucketWebsite
GetChannelMembershipPreferences	Gewährt die Berechtigung, alle Einstellungen zu einer Kanalmitgliedschaft zu erhalten	Lesen	app-instance-bot* app-instance-user*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			channel*		
GetChannelMessage	Gewährt die Berechtigung, alle Details zu einer Nachricht in einem Kanal zu erhalten	Lesen	app-instance-bot*		
			app-instance-user*		
			channel*		
GetChannelMessageStatus	Gewährt die Berechtigung, den Status zu einer Nachricht in einem Kanal zu erhalten	Lesen	app-instance-bot*		
			app-instance-user*		
			channel*		
GetDomain	Gewährt die Berechtigung zum Abrufen der Domain-Details einer Domain, die dem Amazon-Chime-Konto zugeordnet ist.	Read			
GetEventsConfiguration	Gewährt die Berechtigung zum Abrufen von Details für eine Events-Konfiguration, sodass ein Bot ausgehende Ereignisse empfangen kann.	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetGlobalSettings	Gewährt die Berechtigung zum Abrufen globaler Einstellungen im Zusammenhang mit Amazon Chime für das AWS-Konto.	Read			
GetMediaCapturePipeline	Gewährt die Berechtigung zum Abrufen einer bestehenden Pipeline zur Medienerfassung.	Lesen	media-pipeline*		
GetMediaInsightsPipelineConfiguration	Gewährt die Berechtigung zum Abrufen einer Pipelinekonfiguration zu Medienerkenntnissen	Lesen	media-insights-pipeline-configuration*		
GetMediaPipeline	Gewährt die Berechtigung zum Abrufen einer bestehenden Medien-Pipeline	Lesen	media-pipeline*		
GetMediaPipelineKinesisVideoStreamPool	Gewährt die Berechtigung zum Abrufen einer bestehenden Medien-Pipeline	Lesen	media-pipeline-kinesis-video-stream-pool*		
GetMeeting	Gewährt die Berechtigung zum Abrufen des Meeting-Datensatzes für eine angegebene Meeting-ID.	Read	meeting*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetMeetingDetail	Gewährt die Berechtigung zum Abrufen von Teilnehmer-, Verbindungs- und anderen Daten für ein Meeting.	Read			
GetMessagingSessionEndpoint	Gewährt die Berechtigung, den Endpunkt für die Messaging-Sitzung zu erhalten	Lesen			
GetMessagingStreamingConfigurations	Gewährt die Berechtigung zum Löschen von Datenstrom-Konfigurationen einer AppInstance	Lesen	app-instance*		
GetPhoneNumber	Gewährt die Berechtigung zum Abrufen von Details zur angegebenen Telefonnummer.	Read			
GetPhoneNumberOrder	Gewährt die Berechtigung zum Abrufen von Details zur angegebenen Telefonnummernbeantragung.	Read			
GetPhoneNumberSettings	Gewährt die Berechtigung zum Abrufen von Telefonnummereinstellungen für Amazon Chime für das AWS-Konto.	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetProxySession	Gewährt die Berechtigung zum Abrufen von Details zur angegebenen Proxykonfiguration für den angegebenen Amazon Chime Voice Connector.	Lesen	voice-connector*		
GetRetentionSettings	Gewährt die Berechtigung zum Abrufen von Kontoeinstellungen für die angegebene Amazon-Chime-Konto-ID.	Lesen			
GetRoom	Gewährt die Berechtigung zum Abrufen eines Raums.	Read			
GetSipMediaApplication	Gewährt die Berechtigung, Details zu einer Amazon-Chime-SIP-Medienanwendung unter dem AWS-Konto des Administrators abzurufen.	Lesen	sip-media-application*		
GetSipMediaApplicationAlexaSkillConfiguration	Gewährt die Berechtigung, die Einstellungen zur Alexa Skill-Konfiguration für eine Amazon-Chime-SIP-Medienanwendung unter dem AWS-Konto des Administrators abzurufen.	Lesen	sip-media-application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetSipMediaApplicationLoggingConfiguration	Gewährt die Berechtigung, die Einstellungen zur Protokollierungskonfiguration für eine Amazon-Chime-SIP-Medienanwendung unter dem AWS-Konto des Administrators abzurufen.	Read	sip-media-application*		
GetSipRule	Gewährt die Berechtigung, Details zu einer Amazon-Chime-SIP-Regel unter dem AWS-Konto des Administrators zu erhalten.	Lesen			
GetSpeakerSearchTask	Gewährt die Berechtigung zum Abrufen einer Rednersuchaufgabe für die angegebene Amazon-Chime-Ressource	Lesen	media-pipeline		
			voice-connector		
GetTelephonyLimits	Gewährt die Berechtigung zum Abrufen von Telefonielimits für das angegebene AWS-Konto.	Read			
GetUser	Gewährt die Berechtigung zum Abrufen von Details zur angegebenen Benutzer-ID.	Read			
GetUserActivityReportData	Gewährt die Berechtigung, eine Zusammenfassung der Benutzeraktivitäten auf der Benutzerdetailseite abzurufen.	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetUserByEmail	Gewährt die Berechtigung zum Abrufen der Benutzerdetails für einen Amazon-Chime-Benutzer basierend auf der E-Mail-Adresse in einem Amazon-Chime-Enterprise- oder Team-Konto.	Read			
GetUserSettings	Gewährt die Berechtigung zum Abrufen von Benutzereinstellungen in Bezug auf den angegebenen Amazon-Chime-Benutzer.	Read			
GetVoiceConnector	Gewährt die Berechtigung zum Abrufen von Details zum angegebenen Amazon Chime Voice Connector.	Read	voice-connector*		
GetVoiceConnectorEmergencyCallingConfiguration	Gewährt die Berechtigung zum Abrufen von Details zur Notrufkonfiguration für den angegebenen Amazon Chime Voice Connector.	Read	voice-connector*		
GetVoiceConnectorGroup	Gewährt die Berechtigung zum Abrufen von Details für die angegebene Amazon Chime Voice Connector-Gruppe.	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetVoiceConnectorLoggingConfiguration	Gewährt die Berechtigung zum Abrufen von Details zur Protokollierungskonfiguration für den angegebenen Amazon Chime Voice Connector.	Read	voice-connector*		
GetVoiceConnectorOrigination	Gewährt die Berechtigung zum Abrufen von Details der Ursprungseinstellungen für den angegebenen Amazon Chime Voice Connector.	Read	voice-connector*		
GetVoiceConnectorProxy	Gewährt die Berechtigung zum Abrufen von Details zur Proxykonfiguration für den angegebenen Amazon Chime Voice Connector.	Read	voice-connector*		
GetVoiceConnectorStreamingConfiguration	Gewährt die Berechtigung zum Abrufen von Details zur Streaming-Konfiguration für den angegebenen Amazon Chime Voice Connector.	Read	voice-connector*		
GetVoiceConnectorTermination	Gewährt die Berechtigung zum Abrufen von Details zu den Beendigungseinstellungen für den angegebenen Amazon Chime Voice Connector.	Read	voice-connector*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetVoiceConnectorTerminationHealth	Gewährt die Berechtigung zum Abrufen der Details des Beendigungszustands für den angegebenen Amazon Chime Voice Connector.	Lesen	voice-connector*		
GetVoiceProfile	Gewährt die Berechtigung zum Abrufen eines Sprachprofils	Lesen	voice-profile*		
GetVoiceProfileDomain	Gewährt die Berechtigung zum Abrufen einer Sprachprofil-Domain	Lesen	voice-profile-domain*		
GetVoiceToneAnalysisTask	Gewährt die Berechtigung zum Abrufen einer Sprachtonanalyseaufgabe für die angegebene Amazon-Chime-Ressource	Lesen	media-pipeline voice-connector		
InviteDelegate	Gewährt die Berechtigung zum Senden einer Einladung zum Akzeptieren der Anforderung einer AWS-Konto-Delegierung für ein Amazon-Chime-Konto.	Write			
InviteUsers	Gewährt die Berechtigung zum Einladen von bis zu 50 Benutzern in das angegebene Amazon-Chime-Konto.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
InviteUsersFromProvider	Gewährt die Berechtigung, Benutzer von einem Drittanbieter auf Ihr Amazon-Chime-Konto einzuladen.	Write			
ListAccountUsageReportData	Gewährt die Berechtigung zum Auflisten der Nutzungsberichtdaten für ein Amazon-Chime-Konto.	List			
ListAccounts	Gewährt die Berechtigung zum Auflisten des Amazon-Chime-Kontos im AWS-Konto des Administrators.	List			
ListApiKeys	Gewährt die Berechtigung zum Auflisten der für das Amazon-Chime-Konto und die Okta-Konfiguration definierten SCIM-Zugriffsschlüssel.	List			
ListAppInstanceAdmins	Gewährt die Berechtigung zum Auflisten von Administratoren in der App-Instance	Auflisten	app-instance*		
			app-instance-bot*		
			app-instance-user*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAppInstanceBots	Gewährt die Berechtigung zum Auflisten aller AppInstanceBots, die unter einer App-Instance erstellt wurden	Auflisten	app-instance-bot*		
ListAppInstanceUserEndpoints	Gewährt die Berechtigung zum Auflisten der Endpunkte, die für einen App-Instance-Benutzer registriert sind	Auflisten	app-instance-user*		
ListAppInstanceUsers	Gewährt die Berechtigung, alle AppInstanceUsers aufzulisten, die unter einer App-Instance erstellt wurden	List	app-instance-user*		
ListAppInstances	Gewährt die Berechtigung, alle Amazon-Chime-App-Instances aufzulisten, die unter einem AWS-Konto erstellt wurden.	List	app-instance*		
ListAttendeeTags	Gewährt die Berechtigung zum Auflisten der Tags, die auf eine Amazon Chime SDK-Teilnehmerressource angewendet werden.	List	meeting*		
ListAttendees	Gewährt die Berechtigung zum Auflisten von bis zu 100 Teilnehmern für ein bestimmtes Amazon Chime SDK-Meeting.	Auflisten	meeting*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAvailableVoiceConnectorRegions	Gewährt die Berechtigung zum Auflisten der verfügbaren AWS-Regionen. Dort können Sie einen Amazon Chime SDK Voice Connector erstellen.	Auflisten			
ListBots	Gewährt die Berechtigung zum Auflisten der Bots, die dem Amazon Chime Enterprise-Konto des Administrators zugeordnet sind.	List			
ListCDRBucket	Gewährt die Berechtigung zum Auflisten von S3 Bucket für Anrufdetailakten.	List			s3:ListAllMyBuckets s3:ListBucket
ListCallingRegions	Gewährt die Berechtigung zum Auflisten der für das AWS-Konto des Administrators verfügbaren Anrufregionen.	Auflisten			
ListChannelBans	Gewährt die Berechtigung zum Auflisten aller Benutzer und Bots, die für einen bestimmten Kanal gesperrt sind	Auflisten	app-instance-bot*		
			app-instance-user*		
			channel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListChannelFlows	Gewährt die Berechtigung, alle Kanal-Flows aufzulisten, die unter einer Chime-App Instance erstellt wurden	Auflisten	channel-flow*		
ListChannelMemberships	Gewährt die Berechtigung, alle Mitgliedschaften für einen Kanal aufzulisten	Auflisten	app-instance-bot*		
			app-instance-user*		
			channel*		
ListChannelMembershipsForAppInstanceUser	Gewährt die Berechtigung zum Auflisten aller Kanäle, denen ein bestimmter Benutzer oder Bot angehört	Auflisten	app-instance-bot*		
			app-instance-user*		
ListChannelMessages	Gewährt die Berechtigung, alle Nachrichten in einem Kanal aufzulisten	Lesen	app-instance-bot*		
			app-instance-user*		
			channel*		
ListChannelModerators	Gewährt die Berechtigung, alle Moderatoren für einen Kanal aufzulisten	List	app-instance-bot*		
			app-instance-user*		
			channel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListChannels	Gewährt die Berechtigung, alle Kanäle aufzulisten, die unter einer Chime-AppInstance erstellt wurden	Auflisten	app-instance-bot*		
			app-instance-user*		
ListChannelsAssociatedWithChannelFlow	Gewährt die Berechtigung, alle Kanäle aufzulisten, die einem Chime-Kanal-Flow zugeordnet sind	Auflisten	channel-flow*		
ListChannelsModeratedByAppInstanceUser	Gewährt die Berechtigung zum Auflisten aller von einem Benutzer oder Bot moderierten Kanäle	Auflisten	app-instance-bot*		
			app-instance-user*		
ListDelegates	Gewährt die Berechtigung zum Auflisten der Konto-Delegierungsinformationen, die dem Amazon-Chime-Konto zugeordnet sind.	List			
ListDirectories	Gewährt die Berechtigung zum Auflisten von Active Directories, die im Directory Service des AWS-Kontos gehostet werden.	List			
ListDomains	Gewährt die Berechtigung zum Auflisten von Domains, die dem Amazon-Chime-Konto zugeordnet sind.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListGroups	Gewährt die Berechtigung zum Auflisten von Active Directory- oder Okta-Benutzergruppen, die dem Amazon Chime Enterprise-Konto zugeordnet sind.	List			
ListMediaCapturePipelines	Gewährt die Berechtigung zum Auflisten von Pipelines zur Medienerfassung.	Auflisten			
ListMediaInsightsPipelineConfigurations	Gewährt die Berechtigung zum Auflisten aller Pipelinekonfigurationen zu Medienerkenntnissen	Auflisten			
ListMediaPipelineKinesisVideoStreamPools	Gewährt die Berechtigung zum Auflisten von Medien-Pipelines	Auflisten			
ListMediaPipelines	Gewährt die Berechtigung zum Auflisten von Medien-Pipelines	Auflisten			
ListMeetingEvents	Gewährt die Berechtigung zum Auflisten aller Ereignisse, die für ein angegebenes Meeting aufgetreten sind.	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListMeetingTags	Gewährt die Berechtigung zum Auflisten der Tags, die auf eine Amazon Chime SDK-Besprechungsressource angewendet werden.	Auflisten	meeting*		
ListMeetings	Gewährt die Berechtigung zum Auflisten von bis zu 100 aktiven Amazon-Chime-SDK-Meetings.	List			
ListMeetingsReportData	Gewährt die Berechtigung zum Auflisten der Meetings, die im angegebenen Zeitraum beendet wurden.	List			
ListPhoneNumberOrders	Gewährt die Berechtigung zum Auflisten der Telefonnummernbestellungen im AWS-Konto des Administrators.	List			
ListPhoneNumbers	Gewährt die Berechtigung zum Auflisten der Telefonnummern im AWS-Konto des Administrators.	List			
ListProxySessions	Gewährt die Berechtigung zum Auflisten von Proxysitzungen für den angegebenen Amazon Chime Voice Connector.	List	voice-connector*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListRoomMemberships	Gewährt die Berechtigung zum Auflisten aller Raummitglieder.	List			
ListRooms	Gewährt die Berechtigung zum Auflisten von Räumen.	List			
ListSipMediaApplications	Gewährt die Berechtigung zum Auflisten aller Amazon-Chime-SIP-Medienanwendungen unter dem AWS-Konto des Administrators.	List			
ListSipRules	Gewährt die Berechtigung zum Auflisten aller Amazon-Chime-SIP-Regeln unter dem AWS-Konto des Administrators.	Auflisten	sip-media-application		
ListSubChannels	Gewährt die Berechtigung, alle SubKanäle unter einem Kanal aufzulisten	Auflisten	app-instance-bot*		
			app-instance-user*		
			channel*		
ListSupportedPhoneNumberCountries	Gewährt die Berechtigung zum Auflisten der vom AWS-Konto unterstützten Telefonnummernländer.	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags, die auf eine Amazon-Chime-Ressource angewendet wurden	Lesen	app-instance		
			app-instance-bot		
			app-instance-user		
			channel		
			channel-flow		
			media-insights-pipeline-configuration		
			media-pipeline		
			media-pipeline-kinesis-video-stream-pool		
			meeting		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			sip-media-application		
			voice-connector		
			voice-profile-domain		
ListUsers	Gewährt die Berechtigung zum Auflisten von Benutzern, die zum angegebenen Amazon-Chime-Konto gehören.	List			
ListVoiceConnectorGroups	Gewährt die Berechtigung zum Auflisten der Amazon Chime Voice Connector-Gruppen im AWS-Konto des Administrators.	List			
ListVoiceConnectorTerminationCredentials	Gewährt die Berechtigung zum Auflisten der SIP-Beendigungsanmeldeinformationen für den angegebenen Amazon Chime Voice Connector.	List	voice-connector*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListVoiceConnectors	Gewährt die Berechtigung zum Auflisten der Amazon Chime Voice Connectors im AWS-Konto des Administrators.	Auflisten			
ListVoiceProfileDomains	Gewährt die Berechtigung zum Auflisten von Sprachprofil-Domains	Auflisten			
ListVoiceProfiles	Gewährt die Berechtigung zum Auflisten von Sprachprofilen	Auflisten	voice-profile-domain*		
LogoutUser	Gewährt die Berechtigung zum Abmelden des angegebenen Benutzers von allen Geräten, bei dem er derzeit angemeldet ist.	Write			
PutAppInstanceRetentionSettings	Gewährt die Berechtigung, Datenaufbewahrung für die App-Instance zu aktivieren	Write	app-instance*		
PutAppInstanceStreamingConfigurations	Gewährt die Berechtigung zum Konfigurieren von Datenstreaming für die App-Instance	Schreiben	app-instance*		
PutAppInstanceUserExpirationSettings	Gewährt die Berechtigung zum Einrichten von Ablaufeinstellungen für einen AppInstanceUser	Schreiben	app-instance-user*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutChannelExpirationSettings	Gewährt die Berechtigung zum Einrichten von Ablaufeinstellungen für einen Kanal	Schreiben	app-instance-user*		
			channel*		
PutChannelMembershipPreferences	Gewährt die Berechtigung, alle Einstellungen zu einer Kanalmitgliedschaft abzulegen	Schreiben	app-instance-bot*		
			app-instance-user*		
			channel*		
PutEventsConfiguration	Gewährt die Berechtigung zum Aktualisieren von Details für eine Events-Konfiguration, sodass ein Bot ausgehende Ereignisse empfangen kann.	Schreiben			
PutMessagingStreamingConfigurations	Gewährt die Berechtigung zum Einrichten von Datenstrom-Konfigurationen für eine AppInstance	Schreiben	app-instance*		
PutRetentionSettings	Gewährt die Berechtigung zum Aktualisieren der Einstellungen für das angegebene Amazon-Chime-Konto.	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutSipMediaApplicationAlexaSkillConfiguration	Gewährt die Berechtigung, die Einstellungen zur Alexa Skill-Konfiguration für eine Amazon-Chime-SIP-Medienanwendung unter dem AWS-Konto des Administrators abzurufen.	Schreiben	sip-media-application*		
PutSipMediaApplicationLoggingConfiguration	Gewährt die Berechtigung, die Einstellungen zur Protokollierungskonfiguration für eine Amazon-Chime-SIP-Medienanwendung unter dem AWS-Konto des Administrators zu aktualisieren.	Write	sip-media-application*		
PutVoiceConnectorEmergencyCallingConfiguration	Gewährt die Berechtigung zum Hinzufügen einer Notrufkonfiguration für den angegebenen Amazon Chime Voice Connector.	Write	voice-connector*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutVoiceConnectorLoggingConfiguration	Gewährt die Berechtigung zum Hinzufügen der Protokollierungskonfiguration für den angegebenen Amazon Chime Voice Connector.	Write	voice-connector*		logs:CreateLogDelivery logs:CreateLogGroup logs:DeleteLogDelivery logs:DescribeLogGroups logs:GetLogDelivery logs:ListLogDeliveries
PutVoiceConnectorOrigination	Gewährt die Berechtigung zum Aktualisieren der Ursprungseinstellungen für den angegebenen Amazon Chime Voice Connector.	Write	voice-connector*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutVoiceConnectorProxy	Gewährt die Berechtigung zum Hinzufügen der Proxykonfiguration für den angegebenen Amazon Chime Voice Connector.	Write	voice-connector*		
PutVoiceConnectorStreamingConfiguration	Gewährt die Berechtigung zum Hinzufügen einer Streaming-Konfiguration für den angegebenen Amazon Chime Voice Connector.	Write	voice-connector*		chime:GetMediaInsightsPipelineConfiguration
			media-insights-pipeline-configuration		
PutVoiceConnectorTermination	Gewährt die Berechtigung zum Aktualisieren der Beendigungseinstellungen für den angegebenen Amazon Chime Voice Connector.	Write	voice-connector*		
PutVoiceConnectorTerminationCredentials	Gewährt die Berechtigung zum Hinzufügen von SIP-Beendigungsanmeldeinformationen für den angegebenen Amazon Chime Voice Connector.	Write	voice-connector*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RedactChannelMessage	Gewährt die Berechtigung, Nachrichteninhalte zu redigieren	Schreiben	app-instance-bot*		
			app-instance-user*		
			channel*		
RedactConversationMessage	Schwärzt die angegebene Chime-Konversationsnachricht.	Schreiben			
RedactRoomMessage	Schwärzt die angegebene Chime Room-Nachricht.	Schreiben			
RegenerateSecurityToken	Gewährt die Berechtigung zum Regenerieren des Sicherheits-Tokens für den angegebenen Bot.	Schreiben			
RegisterAppInstanceUserEndpoint	Gewährt die Berechtigung zum Registrieren eines Endpunkts für einen App-Instance-Benutzer	Schreiben	app-instance-user*		mobiletargeting:GetApp
RenameAccount	Gewährt die Berechtigung zum Ändern des Kontonamens für das Amazon Chime Enterprise- oder Team-Konto.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RenewDelegate	Gewährt die Berechtigung zum Erneuern der Delegierungsanforderung, die einem Amazon-Chime-Konto zugeordnet ist.	Write			
ResetAccountResource	Gewährt die Berechtigung zum Zurücksetzen der Konto-Ressource in Ihrem Amazon-Chime-Konto.	Write			
ResetPersonalPIN	Gewährt die Berechtigung zum Zurücksetzen der Meeting-PIN des angegebenen Benutzers in einem Amazon-Chime-Konto.	Write			
RestorePhoneNumber	Gewährt die Berechtigung zum Wiederherstellen der angegebenen Telefonnummer aus der Löschwarteschlange im Telefonnummernverzeichnis.	Write			
RetrieveDataExports	Gewährt die Berechtigung zum Download der von der Aktion „Anhänge anfordern“ zurückgegebenen Datei mit den Links auf alle Benutzeranhänge.	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SearchAvailablePhoneNumbers	Gewährt die Berechtigung zum Suchen von Telefonnummern, die vom Netzbetreiber bestellt werden können.	Lesen			
SearchChannels	Erteilt die Berechtigung zum Durchsuchen von Kanälen, denen ein AppInstanceUser angehört, oder zum Durchsuchen von Kanälen innerhalb der AppInstance für einen AppInstaceAdmin	Auflisten	app-instance-bot*		
			app-instance-user*		
SendChannelMessage	Gewährt die Berechtigung, eine Nachricht an einen bestimmten Kanal zu senden, dem das Mitglied angehört	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
StartDataExport	Gewährt die Berechtigung zum Senden der Anforderung „Anhänge anfordern“.	Schreiben			
StartMeetingTranscription	Gewährt die Berechtigung zum Starten einer Transkription für eine Besprechung	Schreiben			
StartSpeakerSearchTask	Gewährt die Berechtigung zum Starten einer Rednersuchaufgabe für die angegebene Amazon-Chime-Ressource	Schreiben	media-pipeline		
			voice-connector		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartVoiceToneAnalysisTask	Gewährt die Berechtigung zum Starten einer Sprachton analyseaufgabe für die angegebene Amazon-Chime-Ressource	Schreiben	media-pipeline		
			voice-connector		
StopMeetingTranscription	Gewährt die Berechtigung zum Beenden einer Besprechung	Schreiben			
StopSpeakerSearchTask	Gewährt die Berechtigung zum Stoppen einer Rednersuchaufgabe für die angegebene Amazon-Chime-Ressource	Schreiben	media-pipeline		
			voice-connector		
StopVoiceToneAnalysisTask	Gewährt die Berechtigung zum Stoppen einer Sprachton analyseaufgabe für die angegebene Amazon-Chime-Ressource	Schreiben	media-pipeline		
			voice-connector		
SubmitSupportRequest	Gewährt die Berechtigung zum Senden einer Kundenservice-Support-Anforderung.	Write			
SuspendUsers	Gewährt die Berechtigung zum Aussetzen von Benutzern in einem Amazon Chime Enterprise-Konto.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagAttendee	Gewährt die Berechtigung, die angegebenen Tags auf den angegebenen Amazon Chime SDK-Teilnehmer anzuwenden.	Markierung	meeting*		
TagMeeting	Gewährt die Berechtigung, die angegebenen Tags auf die angegebene Amazon Chime SDK-Besprechung anzuwenden.	Markierung	meeting*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
TagResource	Gewährt die Berechtigung, die angegebenen Tags auf die angegebene Amazon-Chime-Ressource anzuwenden	Markierung	app-instance		
			app-instance-bot		
			app-instance-user		
			channel		
			channel-flow		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			media-insights-pipeline-configuration		
			media-pipeline		
			media-pipeline-kinesis-video-stream-pool		
			meeting		
			sip-media-application		
			voice-connector		
			voice-profile-domain		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UnauthorizeDirectory	Gewährt die Berechtigung, die Autorisierung eines Active Directory für das Amazon Chime Enterprise-Konto aufzuheben.	Schreiben			
UntagAttendee	Gewährt die Berechtigung, die angegebenen Tags vom angegebenen Amazon Chime SDK-Teilnehmer aufzuheben.	Markierung	meeting*		
UntagMeeting	Gewährt die Berechtigung, die angegebenen Tags von der angegebenen Amazon Chime SDK-Besprechung aufzuheben.	Markierung	meeting*		
UntagResource	Gewährt die Berechtigung, die angegebenen Tags aus der angegebenen Amazon-Chime-Ressource zu entfernen	Markierung	app-instance		
			app-instance-bot		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			app-instance-user		
			channel		
			channel-flow		
			media-insights-pipeline-configuration		
			media-pipeline		
			media-pipeline-kinesis-video-stream-pool		
			meeting		
			sip-media-application		
			voice-connector		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			voice-profile-domain		
				aws:TagKeys	
UpdateAccount	Gewährt die Berechtigung zum Aktualisieren der Kontodetails für das angegebene Amazon-Chime-Konto.	Write			
UpdateAccountOpenIdConfig	Gewährt die Berechtigung zum Aktualisieren der OpenIdConfig-Attribute für Ihr Amazon-Chime-Konto.	Write			
UpdateAccountResource	Gewährt die Berechtigung zum Aktualisieren der Konto-Ressource in Ihrem Amazon-Chime-Konto.	Write			
UpdateAccountSettings	Gewährt die Berechtigung zum Aktualisieren der Einstellungen für das angegebene Amazon-Chime-Konto.	Write			
UpdateAppInstance	Gewährt die Berechtigung zum Aktualisieren von AppInstance-Metadaten	Schreiben	app-instance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateAppInstanceBot	Gewährt die Berechtigung zum Aktualisieren der Details für einen AppInstanceBot	Schreiben	app-instance-bot*		
UpdateAppInstanceUser	Gewährt die Berechtigung zum Aktualisieren der Details für einen AppInstanceUser	Schreiben	app-instance-user*		
UpdateAppInstanceUserEndpoint	Gewährt die Berechtigung zum Aktualisieren eines Endpunkts, der für einen App-Instance-Benutzer registriert ist	Schreiben	app-instance-user*		
UpdateAttendeeCapabilities	Gewährt die Berechtigung für die Funktionen, die Sie aktualisieren möchten	Schreiben	meeting*		
UpdateBot	Gewährt die Berechtigung zum Aktualisieren des Status des angegebenen Bots.	Write			
UpdateCDRSettings	Gewährt die Berechtigung zum Aktualisieren des S3 Bucket für Anrufdetailakten.	Write			s3:CreateBucket s3:DeleteBucket s3:ListAllMyBuckets

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateChannel	Gewährt die Berechtigung zum Aktualisieren der Attribute eines Kanals	Schreiben	app-instance-bot*		
			app-instance-user*		
			channel*		
UpdateChannelFlow	Gewährt die Berechtigung zum Aktualisieren eines Kanal-Flows	Schreiben	channel-flow*		
UpdateChannelMessage	Gewährt die Berechtigung, den Inhalt einer Nachricht zu aktualisieren	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
UpdateChannelReadMarker	Gewährt die Berechtigung, den Zeitstempel auf den Zeitpunkt zu setzen, zu dem ein Benutzer zuletzt Nachrichten in einem Kanal gelesen hat	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
UpdateGlobalSettings	Gewährt die Berechtigung zum Aktualisieren der globalen Einstellungen in Bezug Amazon Chime für das AWS-Konto.	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateMediaInsightsPipelineConfiguration	Gewährt die Berechtigung zum Aktualisieren des Status einer Pipelinekonfiguration zu Medienerkenntnissen	Schreiben	media-insights-pipeline-configuration*		chime:ListVoiceConnectors iam:PassRole kinesis:DescribeStream s3:ListBucket
UpdateMediaInsightsPipelineStatus	Gewährt die Berechtigung zum Aktualisieren des Status einer Pipeline zu Medienerkenntnissen	Schreiben	media-pipeline*		
UpdateMediaPipelineKinesisVideoStreamPool	Gewährt die Berechtigung zum Aktualisieren eines Kinesis-Videostreampools	Schreiben	media-pipeline-kinesis-video-stream-pool*		
UpdatePhoneNumber	Gewährt die Berechtigung zum Aktualisieren von Telefonnummerndetails für die angegebene Telefonnummer.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdatePhoneNumberSettings	Gewährt die Berechtigung zum Aktualisieren der Telefonnummereinstellungen für Amazon Chime für das AWS-Konto.	Write			
UpdateProxySession	Gewährt die Berechtigung zum Aktualisieren einer Proxysitzung für den angegebenen Amazon Chime Voice Connector.	Write	voice-connector*		
UpdateRoom	Gewährt die Berechtigung zum Aktualisieren eines Raums.	Write			
UpdateRoomMembership	Gewährt die Berechtigung zum Aktualisieren der Raummitgliedschaftsrolle.	Write			
UpdateSipMediaApplication	Gewährt die Berechtigung, Eigenschaften einer Amazon-Chime-SIP-Medienanwendung unter dem AWS-Konto des Administrators zu aktualisieren.	Write	sip-media-application*		
UpdateSipMediaApplicationCall	Gewährt die Berechtigung zum Aktualisieren einer Amazon-Chime-SIP-Medienanwendung unter dem AWS-Konto des Administrators.	Write	sip-media-application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateSipRule	Gewährt die Berechtigung, Eigenschaften einer Amazon-Chime-SIP-Regel unter dem AWS-Konto des Administrators zu aktualisieren.	Write	sip-media-application		
UpdateSupportedLicenses	Gewährt die Berechtigung zum Aktualisieren der unterstützten Lizenzebenen für Benutzer im Amazon-Chime-Konto.	Write			
UpdateUser	Gewährt die Berechtigung zum Aktualisieren der Benutzerdetails für eine bestimmte Benutzer-ID.	Write			
UpdateUserLicenses	Gewährt die Berechtigung zum Aktualisieren der Lizenzen für die Amazon Chime Benutzer.	Write			
UpdateUserSettings	Gewährt die Berechtigung zum Aktualisieren der Benutzereinstellungen in Bezug auf den angegebene Amazon-Chime-Benutzer.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateVoiceConnector	Gewährt die Berechtigung zum Aktualisieren von Amazon Chime Voice Connector-Details für den angegebenen Amazon Chime Voice Connector.	Write	voice-connector*		
UpdateVoiceConnectorGroup	Gewährt die Berechtigung zum Aktualisieren der Amazon Chime Voice Connector -Gruppendetails für die angegebene Amazon Chime Voice Connector-Gruppe.	Schreiben	voice-connector		
UpdateVoiceProfile	Gewährt die Berechtigung zum Aktualisieren eines Sprachprofils	Schreiben	voice-profile*		
UpdateVoiceProfileDomain	Gewährt die Berechtigung zum Aktualisieren einer Sprachprofil-Domain	Schreiben	voice-profile-domain*		
ValidateAccountResource	Gewährt die Berechtigung zum Validieren der Konto-Ressource im Amazon-Chime-Konto.	Lesen			
ValidateE911Address	Erteilt die Erlaubnis zur Validierung einer Adresse, die für 911-Anrufe mit Amazon Chime Voice Connectors verwendet werden soll	Lesen			

Von Amazon Chime definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
meeting	`arn:${Partition}:chime::${AccountId}:meeting/${MeetingId}`	aws:ResourceTag/${TagKey}
app-instance	`arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}`	aws:ResourceTag/${TagKey}
app-instance-user	`arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}/user/${AppInstanceUserId}`	aws:ResourceTag/${TagKey}
app-instance-bot	`arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}/bot/${AppInstanceBotId}`	aws:ResourceTag/${TagKey}
channel	`arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}/channel/${ChannelId}`	aws:ResourceTag/${TagKey}
channel-flow	`arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}/channel-flow/${ChannelFlowId}`	aws:ResourceTag/${TagKey}
media-pipeline	`arn:${Partition}:chime:${Region}:${AccountId}:media-pipeline/${MediaPipelineId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
media-insights-pipeline-configuration	arn:${Partition}:chime:${Region}:${AccountId}:media-insights-pipeline-configuration/${ConfigurationName}	aws:ResourceTag/${TagKey}
media-pipeline-kinesis-video-stream-pool	arn:${Partition}:chime:${Region}:${AccountId}:media-pipeline-kinesis-video-stream-pool/${PoolName}	aws:ResourceTag/${TagKey}
voice-profile-domain	arn:${Partition}:chime:${Region}:${AccountId}:voice-profile-domain/${VoiceProfileDomainId}	aws:ResourceTag/${TagKey}
voice-profile	arn:${Partition}:chime:${Region}:${AccountId}:voice-profile/${VoiceProfileId}	
voice-connector	arn:${Partition}:chime:${Region}:${AccountId}:vc/${VoiceConnectorId}	aws:ResourceTag/${TagKey}
sip-media-application	arn:${Partition}:chime:${Region}:${AccountId}:sma/${SipMediaApplicationId}	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Chime

Amazon Chime definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Schlüssel eines Tags und den Wert einer Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüsselwertpaaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach den Tag-Schlüsseln in einer Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Clean Rooms

AWS Clean Rooms (Dienstpräfix:`cleanrooms`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Clean Rooms definierte Aktionen
- Von AWS Clean Rooms definierte Ressourcentypen
- Bedingungsschlüssel für AWS Clean Rooms

Von AWS Clean Rooms definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetCollaborat	Erteilt die Berechtigung, Details von AnalysisT	Lesen	analysistemplate*		cleanrooms:GetColl

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ionAnalysisTemplate	emplates einzusehen, die der Zusammenarbeit zugeordnet sind				aboration AnalysisTemplate
			collaboration*		
BatchGetSchema	Gewährt die Berechtigung zum Anzeigen von Details für Schemata	Lesen	collaboration*		cleanrooms:GetSchema
			configuredtableassociation*		
BatchGetSchemaAnalysisRule	Erteilt die Berechtigung zum Anzeigen von Analyseregeln, die mit Schemas verknüpft sind	Lesen	collaboration*		cleanrooms:GetSchema
			configuredtableassociation*		
CreateAnalysisTemplate	Erteilt die Berechtigung zum Erstellen einer neuen Analysevorlage	Schreiben	analysistemplate*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateCollaboration	Gewährt die Berechtigung zum Erstellen einer neuen Zusammenarbeit, einer gemeinsamen Datenzusammentragungsumgebung	Schreiben	collaboration*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateConfiguredAudienceModelAssociation	Gewährt die Berechtigung zum Verknüpfen eines von Cleanrooms ML konfigurierten Zielgruppenmodells mit einer Zusammenarbeit durch Erstellen einer neuen Assoziation	Schreiben	configuredaudiencemodelassociation*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	cleanrooms-ml:GetConfiguredAudienceModel cleanrooms-ml:GetConfiguredAudienceModelPolicy cleanrooms-ml:PutConfiguredAudienceModelPolicy
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateConfiguredTable	Gewährt die Berechtigung zum Erstellen einer neuen konfigurierten Tabelle	Schreiben	configuredtable*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	glue:BatchGetPartition glue:GetDatabase glue:GetDatabases glue:GetPartition glue:GetPartitions glue:GetSchemaVersion glue:GetTable glue:GetTables
CreateConfiguredTableAnalysisRule	Gewährt die Berechtigung zum Erstellen einer Analysegel für eine konfiguriere Tabelle	Schreiben	configuredtable*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateConfiguredTableAssociation	Gewährt die Berechtigung zum Verknüpfen einer konfigurierten Tabelle mit einer Zusammenarbeit, indem eine neue Zuordnung erstellt wird	Schreiben	configuredtable*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	iam:PassRole
			configuredtableassociation*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateMembership	Gewährt die Berechtigung zum Zusammenfügen von Zusammenarbeiten durch Erstellen einer Mitgliedschaft	Schreiben	collaboration*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	iam:PassRole logs:CreateLogDelivery logs:CreateLogGroup logs:DeleteLogDelivery logs:DescribeLogGroups logs:DescribeResourcePolicies logs:GetLogDelivery logs:ListLogDeliveries

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					logs:PutResourcePolicy logs:UpdateLogDelivery s3:GetBucketLocation
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreatePrivacyBudgetTemplate	Gewährt die Berechtigung zum Erstellen einer neuen Vorlage für ein Datenschutzbudget	Schreiben	membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			privacybudgettemplate*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteAnalysisTemplate	Erteilt die Berechtigung zum Löschen einer bestehenden Analysevorlage	Schreiben	analysistemplate*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteCollaboration	Gewährt die Berechtigung zum Löschen einer vorhandenen Zusammenarbeit	Schreiben	collaboration*		cleanrooms-ml:DeleteConfiguredAudienceModelPolicy cleanrooms-ml:GetConfiguredAudienceModelPolicy cleanrooms-ml:PutConfiguredAudienceModelPolicy

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteConfiguredAudienceModelAssociation	Gewährt die Berechtigung zum Löschen einer vorhandenen konfigurierten Zielgruppenmodell-Zuordnung	Schreiben	configuredaudiencemodelassociation*		cleanrooms-ml:DeleteConfiguredAudienceModelPolicy cleanrooms-ml:GetConfiguredAudienceModelPolicy cleanrooms-ml:PutConfiguredAudienceModelPolicy
DeleteConfiguredTable	Gewährt die Berechtigung zum Löschen einer konfigurierten Tabelle	Schreiben	configuredtable*		
DeleteConfiguredTableAnalysisRule	Gewährt die Berechtigung zum Löschen einer vorhandenen Analyseregel	Schreiben	configuredtable*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteConfiguredTableAssociation	Gewährt die Berechtigung zum Entfernen einer konfigurierten Tabellenzuordnung aus einer Zusammenarbeit	Schreiben	configuredtableassociation*		
DeleteMember	Gewährt die Berechtigung zum Löschen von Mitgliedern aus einer Zusammenarbeit	Schreiben	collaboration*		cleanrooms-ml:DeleteConfiguredAudienceModelPolicy cleanrooms-ml:GetConfiguredAudienceModelPolicy cleanrooms-ml:PutConfiguredAudienceModelPolicy
DeleteMembership	Gewährt die Berechtigung zum Verlassen von Zusammenarbeiten durch Löschen einer Mitgliedschaft	Schreiben	membership*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeletePrivacyBudgetTemplate	Gewährt die Berechtigung zum Löschen einer bestehenden Vorlage für ein Datenschutzbudget	Schreiben	privacybudgettemplate*		
GetAnalysisTemplate	Erteilt die Berechtigung zum Anzeigen der Details einer Analysevorlage	Lesen	analysistemplate*		
GetCollaboration	Gewährt die Berechtigung zum Anzeigen von Details für eine Zusammenarbeit	Lesen	collaboration*		
GetCollaborationAnalysisTemplate	Erteilt die Berechtigung zum Anzeigen der Details einer Analysevorlage innerhalb einer Zusammenarbeit	Lesen	analysistemplate*		
			collaboration*		
GetCollaborationConfiguredAudienceModelAssociation	Gewährt die Berechtigung zum Anzeigen von Details für eine konfigurierte Zuordnung eines Zielgruppenmodells innerhalb einer Zusammenarbeit	Lesen	collaboration*		
			configuredaudiencemodelassociation*		
GetCollaborationPrivacyBudgetTemplate	Gewährt die Berechtigung zum Anzeigen der Details einer Vorlage für ein Datenschutzbudget innerhalb einer Zusammenarbeit	Lesen	collaboration*		
			privacybudgettemplate*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetConfiguredAudienceModelAssociation	Gewährt die Berechtigung zum Anzeigen von Details für eine konfigurierte Zuordnung eines Zielgruppenmodells	Lesen	configuredaudiencemodelassociation*		
GetConfiguredTable	Gewährt die Berechtigung zum Anzeigen von Details für eine konfigurierte Tabelle	Lesen	configuredtable*		
GetConfiguredTableAnalysisRule	Gewährt die Berechtigung zum Anzeigen von Analysegeln für eine konfiguriere Tabelle	Lesen	configuredtable*		
GetConfiguredTableAssociation	Gewährt die Berechtigung zum Anzeigen von Details für eine konfigurierte Tabellenzuordnung	Lesen	configuredtableassociation*		
GetMembership	Gewährt die Berechtigung zum Anzeigen von Details zu einer Mitgliedschaft	Lesen	membership*		
GetPrivacyBudgetTemplate	Gewährt die Berechtigung zum Anzeigen der Details einer Vorlage für ein Datenschutzbudget	Lesen	privacybudgettemplate*		
GetProtectedQuery	Gewährt die Berechtigung zum Anzeigen einer Projektabfrage	Lesen	membership*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetSchema	Gewährt die Berechtigung zum Anzeigen von Details für ein Schema	Lesen	collaboration*		
			configuredtableassociation*		
GetSchemaAnalysisRule	Gewährt die Berechtigung zum Anzeigen von mit einem Schema verknüpften Analyseregeln	Lesen	collaboration*		cleanrooms:GetSchema
			configuredtableassociation*		
ListAnalysisTemplates	Erteilt die Berechtigung, verfügbare Analysevorlagen aufzulisten	Auflisten	analysistemplate*		
			membership*		
ListCollaborationAnalysisTemplates	Erteilt die Berechtigung, verfügbare Analysevorlagen innerhalb einer Zusammenarbeit aufzulisten	Auflisten	collaboration*		
ListCollaborationConfiguredAudienceModelAssociations	Gewährt die Berechtigung zum Auflisten einer konfigurierten Zuordnung eines Zielgruppenmodells innerhalb einer Zusammenarbeit	Auflisten	collaboration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListCollaborationPrivacyBudgetTemplates	Gewährt die Berechtigung, verfügbare Analysevorlagen innerhalb eines Datenschutzbudgets aufzulisten	Auflisten	collaboration*		
ListCollaborationPrivacyBudgets	Gewährt die Berechtigung zum Auflisten von Datenschutzbudgets innerhalb einer Zusammenarbeit	Auflisten	collaboration*		
ListCollaborations	Gewährt die Berechtigung zum Auflisten verfügbarer Kollaborationen	Auflisten			
ListConfiguredAudienceModelAssociations	Gewährt die Berechtigung zum Auflisten verfügbarer konfigurierter Zielgruppenmodell-Zuordnungen für eine Mitgliedschaft	Auflisten	configuredaudiencemodelassociation*		
			membership*		
ListConfiguredTableAssociations	Gewährt die Berechtigung zum Auflisten verfügbarer konfigurierter Tabellenzuordnungen für eine Mitgliedschaft	Auflisten	configuredtableassociation*		
			membership*		
ListConfiguredTables	Gewährt die Berechtigung zum Auflisten verfügbarer konfigurierter Tabellen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListMembers	Gewährt die Berechtigung zum Auflisten der Mitglieder einer Zusammenarbeit	Auflisten	collaboration*		
ListMemberships	Gewährt die Berechtigung zum Auflisten verfügbarer Mitgliedschaften	Auflisten			
ListPrivacyBudgetTemplates	Gewährt die Berechtigung, verfügbare Datenschutzbudgets aufzulisten	Auflisten	membership*		
			privacybudgettemplate*		
ListPrivacyBudgets	Gewährt die Berechtigung zum Auflisten verfügbarer Datenschutzbudgets	Auflisten	membership*		
ListProtectedQueries	Gewährt die Berechtigung zum Auflisten von geschützten Abfragen	Auflisten	membership*		
ListSchemas	Gewährt die Berechtigung zum Anzeigen der verfügbaren Schemata für eine Zusammenarbeit	Auflisten	collaboration*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Auflisten	analysistemplate		
			collaboration		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			configuredaudiencemodelassociation		
			configuredtable		
			configuredtableassociation		
			membership		
			privacybudgettemplate		
PreviewPrivacyImpact	Gewährt die Berechtigung, eine Vorschau der Einstellungen für die Datenschutzbudgetvorlage anzuzeigen	Lesen	membership*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartProtectedQuery	Gewährt die Berechtigung zum Starten von geschützten Abfragen	Schreiben	configuredtableassociation*		cleanrooms:GetCollaborationAnalysisTemplate cleanrooms:GetSchema s3:GetBucketLocation s3:ListBucket s3:PutObject
			membership*		
			analysistemplate		
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren	analysistemplate		
			collaboration		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			configuredaudiencemodelassociation		
			configuredtable		
			configuredtableassociation		
			membership		
			privacybudgettemplate		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Tagging	analysistemplate		
			collaboration		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			configuredaudiencemodelassociation		
			configuredtable		
			configuredtableassociation		
			membership		
			privacybudgettemplate		
				aws:TagKeys	
UpdateAnalysisTemplate	Erteilt die Berechtigung, Details der Analysevorlage zu aktualisieren	Schreiben	analysistemplate*		
UpdateCollaboration	Gewährt die Berechtigung zum Aktualisieren der Details der Zusammenarbeit	Schreiben	collaboration*		
UpdateConfiguredAudienceModelAssociation	Gewährt die Berechtigung zum Aktualisieren einer konfigurierten Zuordnung eines Zielgruppenmodells	Schreiben	configuredaudiencemodelassociation*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateConfiguredTable	Gewährt die Berechtigung zum Aktualisieren einer bestehenden konfigurierten Tabelle	Schreiben	configuredtable*		
UpdateConfiguredTableAnalysisRule	Gewährt die Berechtigung zum Aktualisieren von Analyseregeln für eine konfiguriere Tabelle	Schreiben	configuredtable*		
UpdateConfiguredTableAssociation	Gewährt die Berechtigung zum Aktualisieren der Zuordnung einer konfigurierten Tabelle	Schreiben	configuredtableassociation*		iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateMembership	Gewährt die Berechtigung zum Anzeigen der Details einer Mitgliedschaft	Schreiben	membership*		iam:PassRole logs:CreateLogDelivery logs:CreateLogGroup logs:DeleteLogDelivery logs:DescribeLogGroups logs:DescribeResourcePolicies logs:GetLogDelivery logs:ListLogDeliveries

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					logs:PutResourcePolicy logs:UpdateLogDelivery s3:GetBucketLocation
UpdatePrivacyBudgetTemplate	Gewährt die Berechtigung, Details der Datenschutzbudgetvorlage zu aktualisieren	Schreiben	privacybudgettemplate*		
UpdateProtectedQuery	Gewährt die Berechtigung zum Aktualisieren von geschützten Abfragen	Schreiben	membership*		

Von AWS Clean Rooms definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
analysistemplate	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/analysistemplate/${AnalysisTemplateId}	aws:ResourceTag/${TagKey}
collaboration	arn:${Partition}:cleanrooms:${Region}:${Account}:collaboration/${CollaborationId}	aws:ResourceTag/${TagKey}
configuredaudiencemodelassociation	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/configuredaudiencemodelassociation/${ConfiguredAudienceModelAssociationId}	aws:ResourceTag/${TagKey}
configuredtable	arn:${Partition}:cleanrooms:${Region}:${Account}:configuredtable/${ConfiguredTableId}	aws:ResourceTag/${TagKey}
configuredtableassociation	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/configuredtableassociation/${ConfiguredTableAssociationId}	aws:ResourceTag/${TagKey}
membership	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}	aws:ResourceTag/${TagKey}
privacybudgettemplate	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/privacybudgettemplate/${PrivacyBudgetTemplateId}	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Clean Rooms

AWS Clean Rooms definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Clean Rooms ML

AWS Clean Rooms ML (Servicepräfix: `cleanrooms-ml`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Clean Rooms ML definierte Aktionen
- Von AWS Clean Rooms ML definierte Ressourcentypen
- Bedingungsschlüssel für AWS Clean Rooms ML

Von AWS Clean Rooms ML definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAudienceModel	Gewährt die Berechtigung zum Erstellen eines Zielgruppenmodells	Schreiben	trainingdataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfiguredAudienceModel	Gewährt die Berechtigung zum Erstellen eines konfigurierten Zielgruppenmodells	Schreiben	audiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTrainingDataset	Gewährt die Berechtigung zum Erstellen eines Trainingsdatensatzes oder einer Startzielgruppe In Clean Rooms ML handelt es sich beim Trainingsdatensatz um Metadaten, die auf eine Glue-Tabelle verweisen, die während der Zielgruppenmodell-Erstellung nur gelesen werden kann	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteAudienceGenerationJob	Gewährt die Berechtigung, den angegebenen Job zur Zielgruppengenerierung zu löschen, und entfernt alle mit dem Job verknüpften Daten	Schreiben	audiencegenerationjob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAudienceModel	Erteilt die Berechtigung, den angegebenen Job zur Zielgruppengenerierung zu löschen, und entfernt alle mit dem Job verknüpften Daten	Schreiben	audiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfiguredAudienceModel	Gewährt die Berechtigung zum Löschen des angegebenen konfigurierten Zielgruppenmodells	Schreiben	configuredaudiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteConfiguredAudienceModelPolicy	Gewährt die Berechtigung zum Löschen des angegebenen konfigurierten Zielgruppenmodells	Schreiben	configuredaudiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteTrainingDataset	Gewährt die Berechtigung zum Löschen des Trainingsdatensatzes	Schreiben	trainingdataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetAudienceGenerationJob	Gewährt die Berechtigung zum Zurückgeben von Informationen über eine Zielgruppenerstellungsaufgabe	Lesen	audiencegenerationjob*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAudienceModel	Gewährt die Berechtigung zum Zurückgeben von Informationen über ein Zielgruppenmodell	Lesen	audiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetConfiguredAudienceModel	Gewährt die Berechtigung zum Zurückgeben von Informationen über ein konfiguriertes Zielgruppenmodell	Lesen	configuredaudiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetConfiguredAudienceModelPolicy	Gewährt die Berechtigung zum Zurückgeben von Informationen über eine konfigurierte Zielgruppenmodellrichtlinie	Lesen	configuredaudiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetTrainingDataset	Gewährt die Berechtigung zum Zurückgeben von Informationen über einen Trainingsdatensatz	Lesen	trainingdataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListAudienceExportJobs	Gewährt die Berechtigung zum Zurückgeben einer Liste von Export-Aufträgen für die Zielgruppe	Auflisten	audiencegenerationjob		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListAudienceGenerationJobs	Gewährt die Berechtigung zum Zurückgeben einer Liste von Aufträgen zum Generieren von Zielgruppen	Auflisten	configuredaudiencemodel		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAudienceModels	Gewährt die Berechtigung zum Zurückgeben von Zielgruppenmodellen	Auflisten			
ListConfiguredAudienceModels	Gewährt die Berechtigung zum Zurückgeben einer Liste von konfigurierten Zielgruppenmodellen	Auflisten			
ListTagsForResource	Gewährt Berechtigungen zum Zurückgeben einer Liste von Tags für eine bereitgestellte Ressource	Auflisten	audiencegenerationjob		
			audiencemodel		
			configuredaudiencemodel		
			trainingdataset		
				aws:TagKeys aws:ResourceTag/${TagKey}	
ListTrainingDatasets	Gewährt die Berechtigung zum Zurückgeben einer Liste von Trainingsdatensätzen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutConfiguredAudienceModelPolicy	Gewährt die Berechtigung zum Erstellen oder Aktualisieren der Ressourcenrichtlinie für ein konfiguriertes Zielgruppenmodell	Berechtigungsverwaltung	configuredaudiencemodel*		
StartAudienceExportJob	Gewährt die Berechtigung, eine Zielgruppe mit einer bestimmten Größe zu exportieren, nachdem eine Zielgruppe generiert wurde	Schreiben	audiencegenerationjob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartAudienceGenerationJob	Gewährt die Berechtigung zum Starten des Auftrags zur Zielgruppengenerierung	Schreiben	configuredaudiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Markieren einer angegebenen Ressource	Markierung	audiencegenerationjob		
			audiencemodel		
			configuredaudiencemodel		
			trainingdataset		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UnTagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer angegebenen Ressource	Markierung	audiencegenerationjob		
			audiencemodel		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			configuredaudiencemodel		
			trainingdataset		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateConfiguredAudienceModel	Gewährt die Berechtigung zum Aktualisieren eines konfigurierten Zielgruppenmodells	Schreiben	configuredaudiencemodel*		
			audiencemodel		
				aws:RequestTag/${TagKey} aws:TagKeys	

Von AWS Clean Rooms ML definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden

können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
trainingdataset	`arn:${Partition}:cleanrooms-ml:${Region}:${Account}:training-dataset/${ResourceId}`	aws:ResourceTag/${TagKey}
audiencemodel	`arn:${Partition}:cleanrooms-ml:${Region}:${Account}:audience-model/${ResourceId}`	aws:ResourceTag/${TagKey}
configuredaudiencemodel	`arn:${Partition}:cleanrooms-ml:${Region}:${Account}:configured-audience-model/${ResourceId}`	aws:ResourceTag/${TagKey}
audiencegenerationjob	`arn:${Partition}:cleanrooms-ml:${Region}:${Account}:audience-generation-job/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Clean Rooms ML

AWS Clean Rooms ML definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString
cleanrooms-ml:CollaborationId	Filtert den Zugriff nach der Kollaborations-ID für Clean Rooms	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für die AWS Cloud Control API

AWS Cloud Control API (Servicepräfix: `cloudformation`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von der AWS Cloud Control API definierte Aktionen
- Von AWS Cloud Control API definierte Ressourcentypen
- Bedingungsschlüssel für AWS Cloud Control API

Von der AWS Cloud Control API definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelResourceRequest	Gewährt die Berechtigung zum Stornieren von Ressourcenanforderungen in Ihrem Konto	Schreiben			
CreateResource	Gewährt die Berechtigung zum Erstellen von Ressourcen in Ihrem Konto	Schreiben			
DeleteResource	Gewährt die Berechtigung zum Löschen von Ressourcen in Ihrem Konto	Schreiben			
GetResource	Gewährt die Berechtigung zum Erhalten von Ressourcen in Ihrem Konto	Lesen			
GetResourceRequestStatus	Gewährt die Berechtigung zum Erhalten von Ressourcenanforderungen in Ihrem Konto	Lesen			
ListResourceRequests	Gewährt die Berechtigung zum Auflisten von Ressourcenanforderungen in Ihrem Konto	Lesen			
ListResources	Gewährt die Berechtigung zum Auflisten von Ressourcen in Ihrem Konto	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateResource	Gewährt die Berechtigung zum Aktualisieren von Ressourcen in Ihrem Konto	Schreiben			

Von AWS Cloud Control API definierte Ressourcentypen

AWS Cloud Control API unterstützt nicht die Angabe eines Ressourcen-ARN im Element `Resource` einer IAM-Richtlinienanweisung. Um den Zugriff auf AWS Cloud Control API zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Cloud Control API

Cloud Control API besitzt keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungskontextschlüssel für Amazon Cloud Directory

Amazon Cloud Directory (Servicepräfix: `clouddirectory`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Cloud Directory definierte Aktionen
- Von Amazon Cloud Directory definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Cloud Directory

Von Amazon Cloud Directory definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddFacetToObject	Gewährt die Berechtigung zum Hinzufügen eines neuen Facets zu einem Objekt	Schreiben	directory*		
ApplySchema	Gewährt die Berechtigung zum Kopieren der Eingabe eines veröffentlichten Schemas in Directory mit demselben Namen und derselben Version des veröffentlichten Schemas	Schreiben	directory* publishedSchema*		
AttachObject	Gewährt die Berechtigung zum Hinzufügen eines vorhandenen Objekts ein anderes vorhandenes Objekt	Schreiben	directory*		
AttachPolicy	Gewährt die Berechtigung zum Anhängen eines Richtlinienobjekts an jedes andere Objekt	Schreiben	directory*		
AttachToIndex	Gewährt die Berechtigung zum Anhängen des angegebenen Objekts an den angegebenen Index	Schreiben	directory*		
AttachTypedLink	Gewährt die Berechtigung zum Hinzufügen einen typisierten Links zwischen Quell- und Ziel-Objektreferenz	Schreiben	directory*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchRead	Erteilt die Berechtigung zum Ausführen aller Leseoperationen in einem Batch. Jede einzelne Produktion innerhalb BatchRead muss explizit gewährt werden	Lesen	directory*		
BatchWrite	Erteilt die Berechtigung zum Ausführen aller Schreiboperationen in einem Batch. Jede einzelne Produktion innerhalb BatchWrite muss explizit gewährt werden	Schreiben	directory*		
CreateDirectory	Erteilt die Berechtigung zum Erstellen eines Verzeichnisses durch Kopieren des veröffentlichten Schemas in das Verzeichnis	Schreiben	publishedSchema*		
CreateFacet	Gewährt die Berechtigung zum Erstellen eines neuen Facets in einem Schema	Schreiben	appliedSchema*		
			developmentSchema*		
CreateIndex	Gewährt die Berechtigung zum Erstellen eines Index-Objekts	Schreiben	directory*		
CreateObject	Gewährt die Berechtigung zum Erstellen eines Objekts im Verzeichnis	Schreiben	directory*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSchema	Gewährt die Berechtigung zum Erstellen eines neuen Schemas in einem Entwicklungsstatus	Schreiben			
CreateTypedLinkFacet	Gewährt die Berechtigung zum Erstellen eines neuen Typed-Link-Facets in einem Schema	Schreiben	appliedSchema* developmentSchema*		
DeleteDirectory	Gewährt die Berechtigung zum Löschen eines Verzeichnisses. Nur deaktivierte Verzeichnisse können gelöscht werden	Schreiben	directory*		
DeleteFacet	Erteilt die Berechtigung zum Löschen eines bestimmten Facets. Alle mit dem Facet assoziierten Attribute und Regeln werden gelöscht	Schreiben	developmentSchema*		
DeleteObject	Erteilt die Berechtigung zum Löschen eines Objekts und die zugehörigen Attribute	Schreiben	directory*		
DeleteSchema	Gewährt die Berechtigung zum Löschen eines bestimmten Schemas	Schreiben	developmentSchema* publishedSchema*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteTypedLinkFacet	Erteilt die Berechtigung zum Löschen eines bestimmten TypedLink-Facets. Alle mit dem Facet assoziierten Attribute und Regeln werden gelöscht	Schreiben	developmentSchema*		
DetachFromIndex	Gewährt die Berechtigung zum Trennen des angegebenen Objekts vom angegebenen Index	Schreiben	directory*		
DetachObject	Erteilt die Berechtigung zum Trennen eines bestimmten Objekts vom übergeordneten Objekt	Schreiben	directory*		
DetachPolicy	Gewährt die Berechtigung zum Trennen einer Richtlinie von einem Objekt	Schreiben	directory*		
DetachTypedLink	Gewährt die Berechtigung zum Trennen eines bestimmten typisierten Link zwischen Quell- und Ziel-Objektreferenz	Schreiben	directory*		
DisableDirectory	Gewährt die Berechtigung zum Deaktivieren des angegebenen Verzeichnisses	Schreiben	directory*		
EnableDirectory	Gewährt die Berechtigung zum Aktivieren des angegebenen Verzeichnisses	Schreiben	directory*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAppliedSchemaVersion	Erteilt die Berechtigung, die aktuelle angewendete Schemaversion ARN zurückzugeben, einschließlich der verwendeten Nebenversion	Lesen	appliedSchema*		
GetDirectory	Gewährt die Berechtigung zum Abrufen von Metadaten zu einem Verzeichnis	Lesen	directory*		
GetFacet	Erteilt die Berechtigung zum Abrufen von Details des Facets, z. B. Facet-Name, Attribute, Regeln oder ObjectType	Lesen	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
GetLinkAttributes	Erteilt die Berechtigung zum Abrufen von Attributen, die einem typisierten Link zugeordnet sind	Lesen	directory*		
GetObjectAttributes	Erteilt die Berechtigung zum Abrufen von Attributen innerhalb eines Facets ab, die einem Objekt zugeordnet sind	Lesen	directory*		
GetObjectInformation	Gewährt die Berechtigung zum Abrufen von Metadaten eines Objekts	Lesen	directory*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetSchemaAsJson	Erteilt die Berechtigung zum Abrufen einer JSON-Darstellung des Schemas	Lesen	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
GetTypedLinkFacetInformation	Erteilt die Berechtigung zum Zurückgeben von Informationen zur Reihenfolge von Identitätsattributen, die mit bestimmten Facet von typisierten Links verbunden sind	Lesen	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
ListAppliedSchemaArns	Erteilt die Berechtigung zum Auflisten von Schemas, die auf ein Verzeichnis angewendet wurden	Auflisten	directory*		
ListAttachedIndices	Gewährt die Berechtigung zum Auflisten der Indizes, die einem Objekt zugeordnet sind	Lesen	directory*		
ListDevelopmentSchemaArns	Erteilt die Berechtigung zum Abrufen der ARNs von Schemas im Entwicklungsstatus	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDirectories	Erteilt die Berechtigung zum Auflisten von Verzeichnissen, die in einem Konto erstellt wurden	Auflisten			
ListFacetAttributes	Gewährt die Berechtigung zum Abrufen von Attributen, die der Facet zugeordnet sind	Lesen	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
ListFacetNames	Erteilt die Berechtigung zum Abrufen der Namen von Facets, die in einem Schema vorhanden sind	Lesen	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
ListIncomingTypedLinks	Gewährt die Berechtigung zum Zurückgeben einer paginierten Liste aller eingehenden TypedLinks für ein bestimmtes Objekt	Lesen	directory*		
ListIndex	Erteilt die Berechtigung zum Auflisten von Objekten, die an den angegebenen Index angefügt sind	Lesen	directory*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListManagedSchemaArns	Erteilt die Berechtigung zum Auflisten der Hauptversionsfamilien jedes verwalteten Schemas. Wenn ein Hauptversions-ARN als SchemaArn bereitgestellt wird, werden stattdessen die Nebenversionsrevisionen in dieser Familie aufgeführt	Auflisten			
ListObjectAttributes	Erteilt die Berechtigung zum Auflisten aller Attribute, die einem Objekt zugeordnet sind	Lesen	directory*		
ListObjectChildren	Erteilt die Berechtigung zum Zurückgeben einer paginierten Liste untergeordneter Objekte, die einem bestimmten Objekt zugeordnet sind	Lesen	directory*		
ListObjectParentPaths	Erteilt die Berechtigung zum Abrufen aller verfügbaren übergeordneten Pfade für beliebige Objekttypen wie z. B. Knoten, Blatt-, Richtlinien-, Indexobjekt-Knoten	Lesen	directory*		
ListObjectParents	Erteilt die Berechtigung zum Auflisten aller übergeordneten Objekte in Verbindung mit einem bestimmten Objekt in Paginierung auf	Lesen	directory*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListObjectPolicies	Erteilt die Berechtigung zum Zurückgeben von Richtlinien, die einem Objekt in Paginierung zugeordnet sind	Lesen	directory*		
ListOutgoingTypedLinks	Gewährt die Berechtigung zum Zurückgeben einer paginierten Liste aller ausgehenden TypedLinks für ein bestimmtes Objekt	Lesen	directory*		
ListPolicyAttachments	Erteilt die Berechtigung zum Zurückgeben aller ObjectIdentifiers, denen eine bestimmte Richtlinie zugeordnet ist	Lesen	directory*		
ListPublishedSchemaArns	Gewährt die Berechtigung zum Abrufen veröffentlichter Schema-ARNs	Auflisten			
ListTagsForResource	Erteilt die Berechtigung zum Zurückgeben von Tags für eine -Ressource	Lesen	directory*		
ListTypedLinkFacetAttributes	Erteilt die Berechtigung zum Zurückgeben einer paginierten Liste von Attributen, die einem Facet eines typisierten Links zugeordnet sind	Lesen	appliedSchema*		
			developmentSchema*		
			publishedSchema*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTypedLinkFacetNames	Erteilt die Berechtigung zum Zurückgeben einer paginierten Liste typisierter Link-Facet-Namen, die in einem Schema vorhanden sind	Lesen	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
LookupPolicy	Erteilt die Berechtigung zum Auflisten aller Richtlinien aus dem Stammverzeichnis des Verzeichnisses für das angegebene Objekt	Lesen	directory*		
PublishSchema	Erteilt die Berechtigung zum Veröffentlichen eines Entwicklungsschemas mit einer Version	Schreiben	developmentSchema*		
PutSchemaFromJson	Erteilt die Berechtigung zum Aktualisieren eines Schemas mit dem JSON-Upload. Nur für Entwicklungsschemata verfügbar	Schreiben			
RemoveFacetFromObject	Gewährt die Berechtigung zum Entfernen des angegebenen Facets aus dem angegebenen Objekt	Schreiben	directory*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Ressource	Markieren	directory*		
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Ressource	Markierung	directory*		
UpdateFacet	Erteilt die Berechtigung zum Hinzufügen/Aktualisieren/Löschen vorhandener Attribute, Regeln oder ObjectType eines Facets	Schreiben	appliedSchema*		
			developmentSchema*		
UpdateLinkAttributes	Erteilt die Berechtigung zum Aktualisieren der Attribute eines bestimmten typisierten Links. Die zu aktualisierenden Attribute dürfen nicht zur Identität des typisierten Links beitragen, wie durch IdentityAttributeOrder angegeben	Schreiben	directory*		
UpdateObjectAttributes	Erteilt die Berechtigung zum Aktualisieren der Attribute eines bestimmten Objekts	Schreiben	directory*		
UpdateSchema	Gewährt die Berechtigung zum Aktualisieren des Schemanamens mit einem neuen Namen	Schreiben	developmentSchema*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateTypedLinkFacet	Erteilt die Berechtigung zum Hinzufügen/Aktualisieren/Löschen vorhandener Attribute, Regeln und Identitätsattributreihenfolge eines Facets eines typisierten Links	Schreiben	developmentSchema*		
UpgradeAppliedSchema	Erteilt die Berechtigung zum Aktualisieren eines einzelnes Verzeichnisses direkt mit PublishedSchemaArn mit Schemaaktualisierungen in MinorVersion. Abwärtskompatible Nebenversions-Upgrades sind sofort für Reader aller Objekte im Verzeichnis verfügbar	Schreiben	directory* publishedSchema*		
UpgradePublishedSchema	Erteilt die Berechtigung zum Aktualisieren eines veröffentlichten Schemas im Rahmen einer neuen Nebenversions-Revision unter Verwendung des aktuellen Inhalts von DevelopmentSchemaArn	Schreiben	developmentSchema* publishedSchema*		

Von Amazon Cloud Directory definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
appliedSchema	`arn:${Partition}:clouddirectory:${Region}:${Account}:directory/${DirectoryId}/schema/${SchemaName}/${Version}`	
developmentSchema	`arn:${Partition}:clouddirectory:${Region}:${Account}:schema/development/${SchemaName}`	
directory	`arn:${Partition}:clouddirectory:${Region}:${Account}:directory/${DirectoryId}`	
publishedSchema	`arn:${Partition}:clouddirectory:${Region}:${Account}:schema/published/${SchemaName}/${Version}`	

Bedingungsschlüssel für Amazon Cloud Directory

Cloud Directory umfasst keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Cloud Map

AWS Cloud Map (Servicepräfix: `servicediscovery`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.

- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Cloud Map definierte Aktionen
- Von AWS Cloud Map definierte Ressourcentypen
- Bedingungsschlüssel für AWS Cloud Map

Von AWS Cloud Map definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateHttpNamespace	Gewährt die Berechtigung zum Erstellen eines HTTP-Namespace	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreatePrivateDnsNamespace	Gewährt die Berechtigung, einen privaten Namespace auf DNS-Basis zu erstellen, der nur in der angegebenen Amazon-VPC sichtbar ist	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreatePublicDnsNamespace	Gewährt die Berechtigung, einen öffentlichen Namespace auf DNS-Basis zu erstellen, der im Internet sichtbar ist	Write		aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateService	Gewährt die Berechtigung zum Erstellen eines Service	Write	namespace*		
				servicediscovery:NamespaceArn aws:TagKeys aws:RequestTag/${TagKey}	
DeleteNamespace	Gewährt die Berechtigung zum Löschen eines bestimmten Namespace	Write	namespace*		
DeleteService	Gewährt die Berechtigung zum Löschen eines bestimmten Service	Write	service*		
DeregisterInstance	Gewährt die Berechtigung, die Datensätze und ggf. die Zustandsprüfung zu löschen, die Amazon Route 53 für die angegebene Instance erstellt hat	Write	service*		
				servicediscovery:ServiceArn	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DiscoverInstances	Gewährt die Berechtigung, registrierte Instances für einen bestimmten Namespace und Service zu erkennen	Lesen		servicediscovery:NamespaceName servicediscovery:ServiceName	
DiscoverInstancesRevision	Gewährt die Berechtigung zum Erkennen registrierter Instances für einen angegebenen Namespace und Service	Lesen		servicediscovery:NamespaceName servicediscovery:ServiceName	
GetInstance	Gewährt die Berechtigung zum Abrufen von Informationen zu einer bestimmten Instance	Read		servicediscovery:ServiceArn	
GetInstancesHealthStatus	Gewährt die Berechtigung, den aktuellen Zustand („Healthy“, „Unhealthy“ oder „Unknown“) einer oder mehrerer Instances abzurufen	Read		servicediscovery:ServiceArn	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetNamespace	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Namespace	Read	namespace*		
GetOperation	Gewährt die Berechtigung zum Abrufen von Informationen zu einer bestimmten Produktion	Read			
GetService	Gewährt die Berechtigung zum Abrufen der Einstellungen für einen bestimmten Service	Read	service*		
ListInstances	Gewährt die Berechtigung, zusammenfassende Informationen zu den Instances abzurufen, die mit einem bestimmten Service registriert wurden	Lesen		servicediscovery:ServiceArn	
ListNamespaces	Gewährt die Berechtigung zum Abrufen von Informationen zu den Namespaces	Lesen			
ListOperations	Gewährt die Berechtigung zum Auflisten von Produktionen, die den von Ihnen angegebenen Kriterien entsprechen	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListServices	Gewährt die Berechtigung zum Abrufen der Einstellungen für alle Services, die bestimmten Filtern entsprechen	Lesen			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für die angegebene Ressource	Lesen			
RegisterInstance	Gewährt die Berechtigung zum Registrieren einer Instance auf der Basis der Einstellungen in einem bestimmten Service	Write	service*		
				servicediscovery:ServiceArn	
TagResource	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Tags zur angegebenen Ressource	Markieren		aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen eines oder mehrerer Tags aus der angegebenen Ressource	Tagging		aws:TagKeys	
UpdateHttpNamespace	Gewährt die Berechtigung zum Aktualisieren der Einstellungen für einen HTTP-Namespace	Schreiben	namespace*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateInstanceCustomHealthStatus	Gewährt die Berechtigung, den aktuellen Zustand einer Instance mit einer benutzerdefinierten Zustandsprüfung zu aktualisieren	Schreiben		servicediscovery:ServiceArn	
UpdatePrivateDnsNamespace	Gewährt die Berechtigung zum Aktualisieren der Einstellungen für einen privaten DNS-Namespace	Schreiben	namespace*		
UpdatePublicDnsNamespace	Gewährt die Berechtigung zum Aktualisieren der Einstellungen für einen öffentlichen DNS-Namespace	Schreiben	namespace*		
UpdateService	Gewährt die Berechtigung zum Aktualisieren der Einstellungen in einem bestimmten Service	Write	service*		

Von AWS Cloud Map definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
namespace	`arn:${Partition}:servicediscovery:${Region}:${Account}:namespace/${NamespaceId}`	aws:ResourceTag/${TagKey}
service	`arn:${Partition}:servicediscovery:${Region}:${Account}:service/${ServiceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Cloud Map

AWS Cloud Map definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf den Markierungen, die in der Anforderung übergeben werden.	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf den Markierungen, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert Aktionen basierend auf den Tag-Schlüsseln, die in der Anforderung übergeben werden.	ArrayOfString
servicediscovery:NamespaceArn	Filtert den Zugriff durch Angabe des Amazon-Ressourcennamens (ARN) für den zugehörigen Namespace	ARN

Bedingungsschlüssel	Beschreibung	Typ
servicediscovery:NamespaceName	Filtert den Zugriff durch Angabe des Namens des zugehörigen Namespace	Zeichenfolge
servicediscovery:ServiceArn	Filtert den Zugriff durch Angabe des Amazon-Ressourcennamens (ARN) für den zugehörigen Service	ARN
servicediscovery:ServiceName	Filtert den Zugriff durch Angabe des Namens des zugehörigen Service	String

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Cloud9

AWS Cloud9 (Servicepräfix: `cloud9`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Cloud9 definierte Aktionen
- Von AWS Cloud9 definierte Ressourcentypen
- Bedingungsschlüssel für AWS Cloud9

Von AWS Cloud9 definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen.

Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ActivateEC2Remote [nur Berechtigung]	Gewährt die Berechtigung zum Starten der Amazon EC2 Instance, die IhrAWSCloud9 IDE stellt eine Verbindung zu	Schreiben	environment*		
CreateEnvironmentEC2	Gewährt die Berechtigung zum Erstellen einer AWS-Cloud9-Entwicklungsumgebung, startet eine Amazon-Elastic-Compute-Cloud-(Amazon-EC2)-Instance und hostet die Umgebung dann auf der Instance	Schreiben		cloud9:EnvironmentName cloud9:InstanceType cloud9:SubnetId cloud9:UserArn cloud9:OwnerArn aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole
CreateEnvironmentMembership	Gewährt die Berechtigung zum Hinzufügen eines Umgebungsmitglieds zur AWS-Cloud9-Entwicklungsumgebung	Schreiben	environment*		
				cloud9:UserArn	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				cloud9:EnvironmentId cloud9:Permissions	
CreateEnvironmentSSH [nur Berechtigung]	Gewährt die Berechtigung zum Löschen einer AWS-Cloud9-SSH-Entwicklungsumgebung	Schreiben		cloud9:EnvironmentName cloud9:OwnerArn aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironmentToken [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines Authentifizierungstoken, das eine Verbindung zwischen denAWS Cloud9 IDE und die Umgebung des Benutzers	Lesen	environment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteEnvironment	Gewährt die Berechtigung zum Löschen einer AWS-Cloud9-Entwicklungsumgebung Wenn die Umgebung auf einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance gehostet wird, wird auch die Instance beendet.	Schreiben	environment*		iam:CreateServiceLinkedRole
DeleteEnvironmentMembership	Gewährt die Berechtigung zum Löschen eines Umgebungsmitglieds aus einer AWS-Cloud9-Entwicklungsumgebung	Schreiben	environment*		
DescribeEC2Remote [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Details zur Verbindung mit der EC2-Entwicklungsumgebung, einschließlich Host, Benutzer und Port	Lesen	environment*		
DescribeEnvironmentMemberships	Gewährt die Berechtigung zum Abrufen von Informationen zu den Umgebungsmitgliedern einer AWS-Cloud9-Entwicklungsumgebung.	Lesen	environment*		
				cloud9:UserArn cloud9:EnvironmentId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeEnvironmentStatus	Gewährt die Berechtigung zum Abrufen der Statusinformationen für eine AWS-Cloud9-Entwicklungsumgebung	Lesen	environment*		
DescribeEnvironments	Gewährt die Berechtigung zum Abrufen von Informationen zu AWS-Cloud9-Entwicklungsumgebungen	Lesen	environment*		
DescribeSSHRemote [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Details über die Verbindung zur SSH-Entwicklungsumgebung, einschließlich Host, Benutzer und Port	Lesen	environment*		
GetEnvironmentConfig [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Konfigurationsinformationen, die zum Initialisieren der AWS-Cloud9-IDE	Lesen	environment*		
GetEnvironmentSettings [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen derAWSCloud9 IDE-Einstellungen für eine angegebene Entwicklungsumgebung	Lesen	environment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetMembershipSettings [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen derAWSCloud9 IDE-Einstellungen für ein angegebenes Umgebungsmitglied	Lesen	environment*		
GetMigrationExperiences [nur Berechtigung]	Gewährt die Berechtigung, die Migrationserfahrung für einen cloud9-Benutzer abzurufen	Lesen			
GetUserPublicKey [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen des öffentlichen SSH-Schlüssels des Benutzers, der von AWS Cloud9 zur Verbindung mit SSH-Entwicklungsumgebungen	Lesen		cloud9:UserArn	
GetUserSettings [nur Berechtigung]	Gewährt die Berechtigung, die AWS-Cloud9-IDE-Einstellungen für einen angegebenen Benutzer abzurufen	Lesen			
ListEnvironments	Gewährt die Berechtigung zum Abrufen einer Liste mit AWS-Cloud9-Entwicklungsumgebung-IDs	Lesen			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine CloudFront-Ressource	Lesen	environment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyTemporaryCredentialsOnEnvironmentEC2 [nur Berechtigung]	Gewährt die Berechtigung zum SetzenAWSverwaltete temporäre Anmeldeinformationen für die Amazon EC2 Instance, die von derAWSIntegrierte Cloud9 Entwicklungsumgebung (IDE)	Schreiben	environment*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer cloud9-Umgebung	Markierung	environment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer CloudFront-Ressource	Markierung	environment*		
				aws:TagKeys	
UpdateEnvironment	Gewährt die Berechtigung zum Ändern der Einstellungen einer vorhandenen AWS-Cloud9-Entwicklungsumgebung.	Schreiben	environment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateEnvironmentMembership	Gewährt die Berechtigung zum Ändern der Einstellungen eines existierenden Umgebungsmitglieds einer AWS-Cloud9-Entwicklungsumgebung.	Schreiben	environment*		
				cloud9:UserArn cloud9:EnvironmentId cloud9:Permissions	
UpdateEnvironmentSettings [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren desAWSCloud9 IDE-Einstellungen für eine angegebene Entwicklungsumgebung	Schreiben	environment*		
UpdateMembershipSettings [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren desAWSCloud9 IDE-Einstellungen für ein angegebenes Umgebungsmitglied	Schreiben	environment*		
UpdateSSHRemote [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren von Details über die Verbindung zur SSH-Entwicklungsumgebung, einschließlich Host, Benutzer und Port	Schreiben	environment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateUserSettings [nur Berechtigung]	Gewährt die Berechtigung, die IDE-spezifischen Einstellungen eines AWS-Cloud9-Benutzers zu aktualisieren.	Schreiben			
ValidateEnvironmentName [nur Berechtigung]	Gewährt die Berechtigung zum Überprüfen des Umgebungsnamens während der Erstellung einer AWS-Cloud9 Entwicklungsumgebung	Lesen			

Von AWS Cloud9 definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
environment	`arn:${Partition}:cloud9:${Region}:${Account}:environment:${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Cloud9

AWS Cloud9 definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen

zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString
cloud9:EnvironmentId	Filtert den Zugriff nach der AWS-Cloud9-Umgebungs-ID	Zeichenfolge
cloud9:EnvironmentName	Filtert den Zugriff nach dem AWS-Cloud9-Umgebungsnamen	Zeichenfolge
cloud9:InstanceType	Filtert den Zugriff nach dem Instance-Typ der Amazon-EC2-Instance der AWS-Cloud9-Umgebung	Zeichenfolge
cloud9:OwnerArn	Filtert den Zugriff nach dem angegebenen Besitzer-ARN	ARN
cloud9:Permissions	Filtert den Zugriff nach dem Typ der AWS-Cloud9-Berechtigungen	Zeichenfolge
cloud9:SubnetId	Filtert den Zugriff nach der ID des Subnetzes, in dem die AWS-Cloud9-Umgebung erstellt wird	Zeichenfolge
cloud9:UserArn	Filtert den Zugriff nach dem angegebenen Benutzer-ARN	ARN

Aktionen, Ressourcen und Bedingungsschlüssel für AWS CloudFormation

AWS CloudFormation (Dienstpräfix:`cloudformation`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS CloudFormation definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ActivateOrganizationsAccess	Erteilt die Berechtigung zur Aktivierung des vertrauenswürdigen Zugriffs zwischen StackSets und Organizations. Wenn der vertrauenswürdige Zugriff zwischen StackSets und Organizations aktiviert ist, verfügt das Verwaltungskonto über Berechtigungen zum Erstellen und Verwalten StackSets für Ihre Organisation	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ActivateType	Gewährt die Berechtigung, eine öffentliche Drittanbietererweiterung zu aktivieren und sie für die Verwendung in Stack-Vorlagen verfügbar zu machen	Schreiben			
BatchDescribeTypeConfigurations	Erteilt die Berechtigung, Konfigurationsdaten für die angegebenen CloudFormation Erweiterungen zurückzugeben	Lesen			
CancelUpdateStack	Gewährt die Berechtigung zum Abbrechen einer Aktualisierung auf dem angegebenen Stack	Write	stack*		
ContinueUpdateRollback	Gewährt die Berechtigung, das Rollback eines Stacks vom Status UPDATE_ROLLBACK_FAILED zum Status UPDATE_ROLLBACK_COMPLETE fortzusetzen	Write	stack*		
				cloudformation:RoleArn	
CreateChangeSet	Gewährt die Berechtigung zum Erstellen einer Liste von Änderungen für einen Stack	Schreiben	stack*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				cloudformation:ChangeSetName cloudformation:ResourceTypes cloudformation:ImportResourceTypes cloudformation:RoleArn cloudformation:StackPolicyUrl cloudformation:TemplateUrl aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
CreateGeneratedTemplate	Erteilt die Berechtigung, eine Vorlage aus vorhandenen Ressourcen zu erstellen, die noch nicht mit verwaltet wurden CloudFormation	Schreiben			
CreateStack	Gewährt die Berechtigung zum Erstellen eines Stacks gemäß Vorlage	Write	stack*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				cloudformation:ResourceTypes cloudformation:RoleArn cloudformation:StackPolicyUrl cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	
CreateStackInstances	Gewährt die Berechtigung zum Erstellen von Stack-Instances für die angegebenen Konten innerhalb der angegebenen Regionen	Write	stackset*		
			stackset-target		
			type		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys cloudformation:TargetRegion	
CreateStackSet	Gewährt die Berechtigung zum Erstellen eines Stack-Sets gemäß Vorlage	Write		cloudformation:RoleArn cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	
CreateUploadBucket [nur Berechtigung]	Gewährt die Berechtigung, Vorlagen in Amazon-S3-Buckets hochzuladen. Wird nur von der AWS CloudFormation Konsole verwendet und ist in der API-Referenz nicht dokumentiert	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeactivateOrganizationsAccess	Erteilt die Erlaubnis, den vertrauenswürdigen Zugriff zwischen StackSets und Organizations zu deaktivieren. Wenn der vertrauenswürdige Zugriff deaktiviert ist, verfügt das Verwaltungskonto nicht über die Berechtigungen zum Erstellen und Verwalten von serviceverwalteten Diensten StackSets für Ihre Organisation	Schreiben			
DeactivateType	Gewährt die Berechtigung, eine öffentliche Erweiterung zu deaktivieren, die zuvor in diesem Konto und in dieser Region aktiviert wurde	Schreiben			
DeleteChangeSet	Gewährt die Berechtigung zum Löschen des angegebenen Änderungssatzes. Das Löschen von Änderungssätzen stellt sicher, dass niemand den falschen Änderungssatz ausführen kann.	Schreiben	stack*		
				cloudformation:ChangeSetName	
DeleteGeneratedTemplate	Erteilt die Berechtigung zum Löschen einer generierten Vorlage	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteStack	Gewährt die Berechtigung zum Löschen eines angegebenen Stacks	Write	stack*		
				cloudformation:RoleArn	
DeleteStackInstances	Gewährt die Berechtigung zum Löschen von Stack-Instances für die angegebenen Konten in den angegebenen Regionen	Write	stackset*		
			stackset-target		
			type		
				cloudformation:TargetRegion	
DeleteStackSet	Gewährt die Berechtigung zum Löschen eines angegebenen Stack-Sets	Schreiben	stackset*		
DeregisterType	Erteilt die Berechtigung, die Registrierung eines vorhandenen CloudFormation Typs oder einer vorhandenen Typversion aufzuheben	Schreiben			
DescribeAccountLimits	Erteilt die Erlaubnis, die Limits Ihres Kontos abzurufen AWS CloudFormation	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeChangeSet	Gewährt die Berechtigung, die Beschreibung für den angegebenen Änderungssatz zurückzugeben	Lesen	stack*		
				cloudformation:ChangeSetName	
DescribeChangeSetHooks	Gewährt die Berechtigung, die Hook-Aufrufinformationen für den angegebenen Änderungssatz zurückzugeben	Lesen	stack*		
				cloudformation:ChangeSetName	
DescribeGeneratedTemplate	Erteilt die Erlaubnis, eine generierte Vorlage zu beschreiben. Die Ausgabe enthält Details zum Fortschritt der Erstellung einer generierten Vorlage	Lesen			
DescribeOrganizationsAccess	Erteilt die Erlaubnis, Informationen über den OrganizationAccess Status des Kontos zurückzugeben	Lesen			
DescribePublisher	Erteilt die Erlaubnis, Informationen über den Herausgeber einer CloudFormation Erweiterung zurückzugeben	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeResourceScan	Erteilt die Erlaubnis, Details eines Ressourcenscans zu beschreiben	Lesen			
DescribeStackDriftDetectionStatus	Gewährt die Berechtigung, Informationen zu einer Produktion zur Erkennung von Stack-Abweichungen zurückzugeben	Read			
DescribeStackEvents	Gewährt die Berechtigung, alle Stack-bezogenen Ereignisse für einen bestimmten Stack zurückzugeben	Lesen	stack*		
DescribeStackInstance	Erteilt die Berechtigung, die Stack-Instance zurückzugeben, die dem angegebenen Stack-Set und der angegebenen Region zugeordnet ist AWS-Konto	Lesen	stackset*		
DescribeStackResource	Gewährt die Berechtigung, eine Beschreibung der angegebenen Ressource im angegebenen Stack zurückzugeben	Read	stack*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeStackResourceDrifts	Gewährt die Berechtigung, Abweichungsinformationen für die Ressourcen zurückzugeben, die im angegebenen Stack auf Abweichungen überprüft wurden	Lesen	stack*		
DescribeStackResources	Erteilt die Berechtigung, AWS Ressourcenbeschreibungen für laufende und gelöschte Stacks zurückzugeben	Lesen	stack*		
DescribeStackSet	Gewährt die Berechtigung, die Beschreibung des angegebenen Stack-Sets zurückzugeben	Read	stackset*		
DescribeStackSetOperation	Gewährt die Berechtigung, die Beschreibung der angegebenen Stack-Set-Produktion zurückzugeben	Lesen	stackset*		
DescribeStacks	Erteilt die Berechtigung, die Beschreibung für den angegebenen Stapel und für alle Stapel zurückzugeben, wenn sie in Kombination mit der Aktion verwendet wird ListStacks	Auflisten	stack		cloudformation:ListStacks
DescribeType	Erteilt die Erlaubnis, Informationen über den angeforderten CloudFormation Typ zurückzugeben	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeTypeRegistration	Erteilt die Erlaubnis, Informationen über den Registrierungsprozess für einen CloudFormation Typ zurückzugeben	Lesen			
DetectStackDrift	Gewährt die Berechtigung, zu ermitteln, ob sich die aktuelle Konfiguration eines Stacks von der erwarteten Konfiguration, die in der Stack-Vorlage definiert ist, sowie den als Vorlagenparameter angegebenen Werten unterscheidet oder davon abweicht	Read	stack*		
DetectStackResourceDrift	Gewährt die Berechtigung, Informationen dazu zurückzugeben, ob sich die aktuelle Konfiguration eines Stacks von der erwarteten Konfiguration, die in der Stack-Vorlage definiert ist, sowie den als Vorlagenparameter angegebenen Werten unterscheidet oder davon abweicht	Read	stack*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DetectStackSetDrift	Gewährt die Berechtigung, Benutzern zu ermöglichen, Abweichungen in einem Stack-Set und in den zugehörigen Stack-Instances zu ermitteln	Read	stackset*		
EstimateTemplateCost	Gewährt die Berechtigung, die geschätzten monatlichen Kosten einer Vorlage zurückzugeben	Read		cloudformation:TemplateUrl	
ExecuteChangeSet	Gewährt die Berechtigung, einen Stack mit den Eingabedaten zu aktualisieren, die beim Erstellen des angegebenen Änderungssatzes bereitgestellt wurden	Schreiben	stack*		
				cloudformation:ChangeSetName	
GetGeneratedTemplate	Erteilt die Berechtigung zum Abrufen einer generierten Vorlage	Lesen			
GetStackPolicy	Gewährt die Berechtigung, die Stack-Richtlinie für einen bestimmten Stack zurückzugeben	Read	stack*		
GetTemplate	Gewährt die Berechtigung, den Vorlagentext für einen bestimmten Stack zurückzugeben	Read	stack*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetTemplateSummary	Gewährt die Berechtigung, Informationen zu einer neuen oder vorhandenen Vorlage zurückzugeben	Lesen	stack		
			stackset		
				cloudformation:TemplateUrl	
ImportStacksToStackSet	Gewährt die Berechtigung, um Benutzern das Importieren vorhandener Stapel in ein neues oder vorhandenes Stackset zu ermöglichen	Schreiben	stackset*		
ListChangeSets	Gewährt die Berechtigung, die ID und den Status jedes aktiven Änderungssatzes für einen Stack zurückzugeben. AWS CloudFormation Listet beispielsweise Änderungssätze auf, die sich im Status CREATE_IN_PROGRESS oder CREATE_PENDING befinden	Auflisten	stack*		
ListExports	Gewährt die Berechtigung, alle exportierten Ausgabewerte im Konto und in der Region aufzulisten, in der Sie diese Aktion aufrufen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListGeneratedTemplates	Erteilt die Erlaubnis, Ihre generierten Vorlagen in dieser Region aufzulisten	Auflisten			
ListImports	Gewährt die Berechtigung zum Auflisten aller Stacks, die einen exportierten Ausgabewert importieren	Auflisten			
ListResourceScanRelatedResources	Erteilt die Berechtigung, die zugehörigen Ressourcen für eine Liste von Ressourcen aus einem Ressourcenscan aufzulisten. Die Antwort gibt an, ob jede zurückgegebene Ressource bereits verwaltet wird von CloudFormation	Auflisten			
ListResourceScanResources	Erteilt die Berechtigung, die Ressourcen aus einem Ressourcenscan aufzulisten. Die Ergebnisse können nach Ressourcen-ID, Ressourcentyp-Präfix, Tag-Schlüssel und Tag-Wert gefiltert werden	Auflisten			
ListResourceScans	Erteilt die Berechtigung, die Ressourcenscans vom neuesten zum ältesten aufzulisten. Standardmäßig werden bis zu 10 Ressourcenscans zurückgegeben	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListStackInstanceResourceDrifts	Gewährt die Berechtigung, Abweichungsinformationen für die Ressourcen zurückzugeben, die in der angegebenen Stack-Instance auf Abweichungen überprüft wurden	Auflisten	stackset*		
ListStackInstances	Gewährt die Berechtigung, zusammenfassende Informationen zu Stack-Instances zurückzugeben, die dem angegebenen Stack-Set zugeordnet sind	List	stackset*		
ListStackResources	Gewährt die Berechtigung, Beschreibungen aller Ressourcen des angegebenen Stacks zurückzugeben	Auflisten	stack*		
ListStackSetAutoDeploymentTargets	Erteilt die Erlaubnis, zusammenfassende Informationen zu StackSet Auto Deployment Targets zurückzugeben	Auflisten	stackset*		
ListStackSetOperationResults	Gewährt die Berechtigung, zusammenfassende Informationen zu den Ergebnissen einer Stack-Set-Produktion zurückzugeben	List	stackset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListStackSetOperations	Gewährt die Berechtigung, zusammenfassende Informationen zu Produktionen zurückzugeben, die für ein Stack-Set ausgeführt werden	List	stackset*		
ListStackSets	Gewährt die Berechtigung, zusammenfassende Informationen zu Stack-Sets zurückzugeben, die dem Benutzer zugeordnet sind	Auflisten			
ListStacks	Erteilt die Berechtigung, die zusammenfassenden Informationen für Stacks zurückzugeben, deren Status dem angegebenen StackStatusFilter entspricht. Erteilt in Kombination mit der DescribeStacks Aktion die Berechtigung, Beschreibungen für Stapel aufzulisten	Auflisten			
ListTypeRegistrations	Erteilt die Erlaubnis, CloudFormation Registrierungsversuche aufzulisten	Auflisten			
ListTypeVersions	Erteilt die Erlaubnis, Versionen eines bestimmten CloudFormation Typs aufzulisten	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTypes	Erteilt die Berechtigung, verfügbare CloudFormation Typen aufzulisten	Auflisten			
PublishType	Erteilt die Erlaubnis, die angegebene Erweiterung als öffentliche Erweiterung in dieser Region in der CloudFormation Registrierung zu veröffentlichen	Schreiben			
RecordHandlerProgress	Gewährt die Berechtigung, den Fortschritt des Handlers aufzuzeichnen	Schreiben	stack*		
RegisterPublisher	Erteilt die Erlaubnis, ein Konto als Herausgeber von öffentlichen Erweiterungen in der CloudFormation Registrierung zu registrieren	Schreiben			
RegisterType	Erteilt die Erlaubnis, einen neuen CloudFormation Typ zu registrieren	Schreiben			
RollbackStack	Gewährt die Berechtigung, den Stack auf den letzten stabilen Status zurückzusetzen	Schreiben	stack*		
				cloudformation:RoleArn	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SetStackPolicy	Gewährt die Berechtigung zum Festlegen einer Stack-Richtlinie für einen bestimmten Stack	Berechtigungsverwaltung	stack*		
				cloudformation:StackPolicyUrl	
SetTypeConfiguration	Erteilt die Berechtigung, die Konfigurationsdaten für eine registrierte CloudFormation Erweiterung im angegebenen Konto und in der angegebenen Region festzulegen	Schreiben			
SetTypeDefaultVersion	Erteilt die Berechtigung, festzulegen, welche Version eines CloudFormation Typs für CloudFormation Operationen gilt	Schreiben			
SignalResource	Gewährt die Berechtigung, ein Signal mit einem Erfolgs- oder Fehlerstatus an die angegebene Ressource zu senden	Schreiben	stack*		
StartResourceScan	Erteilt die Berechtigung, einen Scan der Ressourcen in diesem Konto in dieser Region zu starten	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopStackSetOperation	Gewährt die Berechtigung, eine laufende Produktion für ein Stack-Set und die zugehörigen Stack-Instances zu stoppen	Write	stackset*		
TagResource	Gewährt die Berechtigung zum Markieren von CloudFormation-Ressourcen	Tagging	changeset		
			stack		
			stackset		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestType	Erteilt die Erlaubnis, eine registrierte Erweiterung zu testen, um sicherzustellen, dass sie alle Anforderungen erfüllt, die für die Veröffentlichung in der CloudFormation Registrierung erforderlich sind	Schreiben			
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung von CloudFormation-Ressourcen	Tagging	changeset		
			stack		
			stackset		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
UpdateGeneratedTemplate	Erteilt die Erlaubnis, eine generierte Vorlage zu aktualisieren. Dies kann verwendet werden, um den Namen zu ändern, Ressourcen hinzuzufügen und zu entfernen, Ressourcen zu aktualisieren DeletionPolicy und die UpdateReplacePolicy Einstellungen zu ändern	Schreiben			
UpdateStack	Gewährt die Berechtigung zum Aktualisieren eines Stacks gemäß Vorlage	Write	stack*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				cloudformation:ResourceTypes cloudformation:RoleArn cloudformation:StackPolicyUrl cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	
UpdateStackInstances	Gewährt die Berechtigung, die Parameterwerte für Stack-Instances in den angegebenen Konten und Regionen zu aktualisieren	Write	stackset*		
			stackset-target		
			type		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				cloudformation:TargetRegion	
UpdateStackSet	Gewährt die Berechtigung zum Aktualisieren eines StackSets gemäß Vorlage	Write	stackset*		
			stackset-target		
			type		
				cloudformation:RoleArn cloudformation:TemplateUrl cloudformation:TargetRegion aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTerminationProtection	Gewährt die Berechtigung zum Aktualisieren des Beendigungsschutzes für den angegebenen Stack	Write	stack*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ValidateTemplate	Gewährt die Berechtigung zur Validierung einer bestimmten Vorlage	Lesen		cloudformation:TemplateUrl	

Von AWS CloudFormation definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
changeset	`arn:${Partition}:cloudformation:${Region}:${Account}:changeSet/${ChangeSetName}/${Id}`	aws:ResourceTag/${TagKey}
stack	`arn:${Partition}:cloudformation:${Region}:${Account}:stack/${StackName}/${Id}`	aws:ResourceTag/${TagKey}
stackset	`arn:${Partition}:cloudformation:${Region}:${Account}:stackset/${StackSetName}:${Id}`	aws:ResourceTag/${TagKey}
stackset-target	`arn:${Partition}:cloudformation:${Region}:${Account}:stackset-target/${StackSetTarget}`	

Ressourcentypen	ARN	Bedingungsschlüssel
type	`arn:${Partition}:cloudformation:${Region}:${Account}:type/resource/${Type}`	
generated template	`arn:${Partition}:cloudformation:${Region}:${Account}:generatedTemplate/${Id}`	
resources can	`arn:${Partition}:cloudformation:${Region}:${Account}:resourceScan/${Id}`	

Bedingungsschlüssel für AWS CloudFormation

AWS CloudFormation definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Bedingungsschlüssel	Beschreibung	Typ
cloudformation:ChangeSetName	Filtert den Zugriff nach einem Namen für AWS CloudFormation den Änderungssatz. Damit können Sie steuern, welche Änderungssätze IAM-Benutzer ausführen oder löschen können.	String
cloudformation:ImportResourceTypes	Filtert den Zugriff nach den Ressourcentypen der Vorlage, z. B. AWS: :EC2: :Instance. Damit können Sie steuern, mit welchen Ressourcentypen IAM-Benutzer arbeiten können, wenn sie eine Ressource in einen Stack importieren möchten.	String
cloudformation:ResourceTypes	Filtert den Zugriff nach den Vorlagenressourcentypen, z. B. AWS: :EC2: :Instance. Steuern Sie hiermit, welche Ressourcentypen IAM-Benutzern zur Verfügung stehen, wenn sie einen Stack erstellen oder aktualisieren.	ArrayOfString
cloudformation:RoleArn	Filtert Zugriff nach dem ARN einer IAM-Servicerolle. Damit können Sie steuern, welche Servicerolle IAM-Benutzer verwenden können, um mit Stacks oder Änderungssätzen zu arbeiten.	ARN
cloudformation:StackPolicyUrl	Filtert Zugriff nach der URL einer Amazon-S3-Stack-Richtlinie. Damit können Sie steuern, welche Stack-Richtlinien IAM-Benutzer einem Stack während einer Aktion zum Erstellen oder Aktualisieren von Stacks zuordnen können.	String
cloudformation:TargetRegion	Filtert den Zugriff nach Stack-Set-Zielregion. Damit können Sie steuern, welche Regionen IAM-Benutzer verwenden können, wenn sie Stack-Sets erstellen oder aktualisieren.	ArrayOfString

Bedingungsschlüssel	Beschreibung	Typ
cloudformation:TemplateUrl	Filtert den Zugriff nach einer Amazon-S3-Vorlagen-URL. Damit können Sie steuern, welche Vorlagen IAM-Benutzer verwenden können, wenn sie Stacks erstellen oder aktualisieren.	String

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CloudFront

Amazon CloudFront (Servicepräfix: `cloudfront`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon CloudFront definierte Aktionen
- Von Amazon CloudFront definierte Ressourcentypen
- Bedingungsschlüssel für Amazon CloudFront

Von Amazon CloudFront definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Associate Alias	Gewährt die Berechtigung zum Zuordnen eines Alias zu einer CloudFront Distribution	Schreiben	distribution*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CopyDistribution	Gewährt die Berechtigung zum Kopieren einer vorhandenen Verteilung und zum Erstellen einer neuen Webverteilung	Schreiben	distribution*		cloudfront:CopyDistribution cloudfront:CreateDistribution cloudfront:GetDistribution
CreateCachePolicy	Gewährt die Berechtigung zum Hinzufügen einer neuen Cache-Richtlinie zu CloudFront	Write	cache-policy*		
CreateCloudFrontOriginAccessIdentity	Gewährt die Berechtigung zum Erstellen einer neuen CloudFront Ursprungszugriffsidentität	Schreiben	origin-access-identity*		
CreateContinuousDeploymentPolicy	Gewährt die Berechtigung zum Hinzufügen einer neuen Richtlinie für die kontinuierliche Bereitstellung zu CloudFront	Schreiben	continuous-deployment-policy*		
CreateDistribution	Gewährt die Berechtigung zum Erstellen einer neuen Webverteilung	Schreiben	distribution*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateFieldLevelEncryptionConfig	Gewährt die Berechtigung zum Erstellen einer neuen Verschlüsselungskonfiguration auf Feldebene	Write			
CreateFieldLevelEncryptionProfile	Gewährt die Berechtigung zum Erstellen eines Verschlüsselungsprofils auf Feldebene	Write			
CreateFunction	Gewährt die Berechtigung zum Erstellen einer CloudFront-Funktion.	Write	function*		
CreateInvalidation	Gewährt die Berechtigung zum Erstellen einer neuen Invalidierungsbatch-Anforderung	Write	distribution*		
CreateKeyGroup	Gewährt die Berechtigung zum Hinzufügen einer neuen Schlüsselgruppe zu CloudFront	Schreiben			
CreateKeyValueStore	Gewährt die Berechtigung zum Erstellen eines CloudFront KeyValueStore	Schreiben	key-value-store*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateMonitoringSubscription	Gewährt die Berechtigung zur Aktivierung zusätzlicher CloudWatch-Metriken für die angegebene CloudFront-Verteilung. Für die zusätzlichen Metriken fallen zusätzliche Kosten an	Schreiben			
CreateOriginAccessControl	Gewährt die Berechtigung zum Erstellen einer neuen Ursprungszugriffssteuerung	Schreiben			
CreateOriginRequestPolicy	Gewährt die Berechtigung zum Hinzufügen einer neuen Ursprungsanforderungsrichtlinie zu CloudFront	Write	origin-request-policy*		
CreatePublicKey	Gewährt die Berechtigung zum Hinzufügen eines neuen öffentlichen Schlüssels zu CloudFront	Write			
CreateRealtimeLogConfig	Gewährt die Berechtigung zum Erstellen einer Echtzeit-Protokollkonfiguration	Schreiben	realtime-log-config*		
CreateResponseHeadersPolicy	Gewährt die Berechtigung zum Hinzufügen einer neuen Antwort-Header-Richtlinie zu CloudFront	Schreiben	response-headers-policy*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSavingsPlan [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines neuen Savings Plan	Schreiben			
CreateStreamingDistribution	Gewährt die Berechtigung zum Erstellen einer neuen RTMP-Distributionskonfiguration	Write	streaming-distribution*		
CreateStreamingDistributionWithTags	Gewährt die Berechtigung zum Erstellen einer neuen RTM-Distributionskonfiguration mit Tags	Schreiben	streaming-distribution*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCachePolicy	Gewährt die Berechtigung zum Löschen einer Cache-Policy	Write	cache-policy*		
DeleteCloudFrontOriginAccessIdentity	Gewährt die Berechtigung zum Löschen einer CloudFront-Ursprungszugriffsidentität	Schreiben	origin-access-identity*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteContinuousDeploymentPolicy	Gewährt die Berechtigung zum Löschen einer Richtlinie für die kontinuierliche Bereitstellung.	Schreiben	continuous-deployment-policy*		
DeleteDistribution	Gewährt die Berechtigung zum Löschen einer Webverteilung	Write	distribution*		
DeleteFieldLevelEncryptionConfig	Gewährt die Berechtigung zum Löschen einer Verschlüsselungskonfiguration auf Feldebene	Write	field-level-encryption-config*		
DeleteFieldLevelEncryptionProfile	Gewährt die Berechtigung zum Löschen eines Verschlüsselungsprofils auf Feldebene	Write	field-level-encryption-profile*		
DeleteFunction	Gewährt die Berechtigung zum Löschen einer CloudFront-Funktion.	Write	function*		
DeleteKeyGroup	Gewährt die Berechtigung zum Löschen einer Schlüsselgruppe	Schreiben			
DeleteKeyValueStore	Gewährt die Berechtigung zum Löschen eines CloudFront KeyValueStore	Schreiben	key-value-store*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteMonitoringSubscription	Diese Aktion deaktiviert zusätzliche CloudWatch-Metriken für die angegebene CloudFront-Verteilung	Schreiben			
DeleteOriginAccessControl	Gewährt die Berechtigung zum Löschen einer Ursprungszugriffssteuerung	Schreiben	origin-access-control*		
DeleteOriginRequestPolicy	Gewährt die Berechtigung zum Löschen einer Ursprungsantragsrichtlinie	Write	origin-request-policy*		
DeletePublicKey	Gewährt die Berechtigung zum Löschen eines öffentlichen Schlüssel von CloudFront	Write			
DeleteRealtimeLogConfig	Gewährt die Berechtigung zum Löschen einer Echtzeit-Protokollkonfiguration	Schreiben	realtime-log-config*		
DeleteResponseHeadersPolicy	Gewährt die Berechtigung zum Löschen einer Antwort-Header-Richtlinie	Schreiben	response-headers-policy*		
DeleteStreamingDistribution	Gewährt die Berechtigung zum Löschen einer RTMP-Verteilung	Write	streaming-distribution*		
DescribeFunction	Gewährt die Berechtigung zum Abrufen einer CloudFront-Funktionszusammenfassung	Lesen	function*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeKeyValueStore	Gewährt die Berechtigung zum Abrufen einer CloudFront-KeyValueStore-Zusammenfassung	Lesen	key-value-store*		
GetCachePolicy	Gewährt die Berechtigung zum Abrufen der Cache-Richtlinie	Read	cache-policy*		
GetCachePolicyConfig	Gewährt die Berechtigung zum Abrufen der Cache-Richtlinienkonfiguration	Read	cache-policy*		
GetCloudFrontOriginAccessIdentity	Gewährt die Berechtigung zum Abrufen der Informationen zu einer CloudFront-Ursprungszugriffsidentität.	Read	origin-access-identity*		
GetCloudFrontOriginAccessIdentityConfig	Gewährt die Berechtigung zum Abrufen der Konfigurationsinformationen zu einer Cloudfront-Ursprungszugriffsidentität.	Lesen	origin-access-identity*		
GetContinuousDeploymentPolicy	Gewährt die Berechtigung zum Abrufen der Richtlinie für die kontinuierliche Bereitstellung	Lesen	continuous-deployment-policy*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetContinuousDeploymentPolicyConfig	Gewährt die Berechtigung zum Abrufen der Richtlinienkonfiguration für die kontinuierliche Bereitstellung	Lesen	continuous-deployment-policy*		
GetDistribution	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Webverteilung	Read	distribution*		
GetDistributionConfig	Gewährt die Berechtigung zum Abrufen von Konfigurationsinformationen über die Verteilung.	Read	distribution*		
GetFieldLevelEncryption	Gewährt die Berechtigung zum Abrufen der Konfigurationsinformationen zur Verschlüsselung auf Feldebene.	Read	field-level-encryption-config*		
GetFieldLevelEncryptionConfig	Gewährt die Berechtigung zum Abrufen der Konfigurationsinformationen zur Verschlüsselung auf Feldebene.	Read	field-level-encryption-config*		
GetFieldLevelEncryptionProfile	Gewährt die Berechtigung zum Abrufen der Konfigurationsinformationen zur Verschlüsselung auf Feldebene.	Read	field-level-encryption-profile*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetFieldLevelEncryptionProfileConfig	Gewährt die Berechtigung zum Abrufen der Konfigurationsinformationen zur Verschlüsselung auf Feldebene.	Read	field-level-encryption-profile*		
GetFunction	Gewährt die Berechtigung zum Abrufen des Codes einer CloudFront-Funktion	Read	function*		
GetInvalidation	Gewährt die Berechtigung zum Abrufen von Informationen über eine Ungültigerklärung	Read	distribution*		
GetKeyGroup	Gewährt die Berechtigung zum Abrufen einer Schlüsselgruppe	Read			
GetKeyGroupConfig	Gewährt die Berechtigung zum Abrufen einer Schlüsselgruppenkonfiguration	Read			
GetMonitoringSubscription	Gewährt die Berechtigung zum Abrufen von Informationen darüber, ob zusätzliche CloudWatch-Metriken für die angegebene CloudFront-Verteilung aktiviert sind.	Lesen			
GetOriginAccessControl	Gewährt die Berechtigung zum Abrufen der Ursprungszugriffssteuerung	Lesen	origin-access-control*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetOriginAccessControlConfig	Gewährt die Berechtigung zum Abrufen der Konfiguration für die Ursprungszugriffssteuerung	Lesen	origin-access-control*		
GetOriginRequestPolicy	Gewährt die Berechtigung zum Abrufen der Ursprungsanforderungsrichtlinie	Read	origin-request-policy*		
GetOriginRequestPolicyConfig	Gewährt die Berechtigung zum Abrufen der Ursprungsanforderungsrichtlinie	Read	origin-request-policy*		
GetPublicKey	Gewährt die Berechtigung zum Abrufen von Informationen über öffentliche Schlüssel	Read			
GetPublicKeyConfig	Gewährt die Berechtigung zum Abrufen von Informationen über Konfiguration öffentlicher Schlüssel.	Read			
GetRealtimeLogConfig	Gewährt die Berechtigung zum Abrufen einer Echtzeit-Protokollkonfiguration	Lesen	realtime-log-config*		
GetResponseHeadersPolicy	Gewährt die Berechtigung zum Abrufen der Antwort-Header-Richtlinie	Lesen	response-headers-policy*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetResponseHeadersPolicyConfig	Gewährt die Berechtigung zum Abrufen der Konfiguration einer Antwort-Header-Richtlinie	Lesen	response-headers-policy*		
GetSavingsPlan [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen eines Savings Plan	Lesen			
GetStreamingDistribution	Gewährt die Berechtigung zum Abrufen von Informationen zu einer RTMP-Verteilung	Read	streaming-distribution*		
GetStreamingDistributionConfig	Gewährt die Berechtigung zum Abrufen der Konfigurationsinformationen zu einer Streaming-Distribution	Read	streaming-distribution*		
ListCachePolicies	Gewährt die Berechtigung zum Auflisten aller Cache-Richtlinien, die in CloudFront für dieses Konto erstellt wurden.	List			
ListCloudFrontOriginAccessIdentities	Gewährt die Berechtigung zum Auflisten Ihrer CloudFront-Ursprungszugriffsidentitäten.	List			
ListConflictingAliases	Gewährt die Berechtigung zum Auflisten aller Aliasse, die mit dem angegebenen Alias in CloudFront in Konflikt stehen	Auflisten	distribution*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListContinuousDeploymentPolicies	Gewährt die Berechtigung zum Auflisten aller Richtlinien für die kontinuierliche Bereitstellung im Konto	Auflisten			
ListDistributions	Gewährt die Berechtigung, alle Verteilungen aufzulisten, die Ihrem AWS-Konto zugeordnet sind	List			
ListDistributionsByCachePolicyId	Gewährt die Berechtigung zum Auflisten der Verteilungs-IDs für Verteilungen, die ein Cache-Verhalten aufweisen, das der angegebenen Cache-Richtlinie zugeordnet ist.	List			
ListDistributionsByKeyGroup	Gewährt die Berechtigung zum Auflisten der Verteilungs-IDs für Verteilungen, die ein Cache-Verhalten aufweisen, das der angegebenen Schlüsselgruppe zugeordnet ist	Auflisten			
ListDistributionsByLambdaFunction [nur Berechtigung]	Gewährt die Berechtigung, alle Verteilungen aufzulisten, die Ihrer Lambda-Funktion zugeordnet sind	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDistributionsByOriginRequestPolicyId	Gewährt die Berechtigung zum Auflisten der Verteilungs-IDs für Verteilungen, die ein Cacheverhalten aufweisen, das der angegebenen Ursprungsanforderungsrichtlinie zugeordnet ist.	List			
ListDistributionsByRealtimeLogConfig	Gewährt die Berechtigung zum Auflisten von Verteilungen, die ein Cache-Verhalten aufweisen, das mit der angegebenen Echtzeit-Protokollkonfiguration verknüpft ist	Auflisten			
ListDistributionsByResponseHeadersPolicyId	Gewährt die Berechtigung zum Auflisten der Verteilungs-IDs für Verteilungen, die ein Cache-Verhalten aufweisen, das der angegebenen Cache-Richtlinie zugeordnet ist	Auflisten			
ListDistributionsByWebACLId	Gewährt die Berechtigung zum Auflisten der mit Ihren AWS-Konto verknüpften Verteilungen mit der angegebenen AWS-WAF-Web-ACL.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListFieldLevelEncryptionConfigs	Gewährt die Berechtigung zum Auflisten aller Verschlüsselungskonfigurationen auf Feldebene, die in CloudFront für dieses Konto erstellt wurden.	List			
ListFieldLevelEncryptionProfiles	Gewährt die Berechtigung zum Auflisten aller Verschlüsselungsprofile auf Feldebene, die in CloudFront für dieses Konto erstellt wurden.	List			
ListFunctions	Gewährt die Berechtigung zum Abrufen einer Liste von CloudFront Funktionen	List			
ListInvalidations	Gewährt die Berechtigung zum Auflisten Ihrer Invalidierungsbatches	List	distribution*		
ListKeyGroups	Gewährt die Berechtigung zum Auflisten aller Schlüsselgruppen, die in CloudFront für dieses Konto erstellt wurden	Auflisten			
ListKeyValueStores	Gewährt die Berechtigung zum Abrufen einer Liste der CloudFront KeyValueStores	Auflisten			
ListOriginAccessControls	Gewährt die Berechtigung zum Auflisten aller Ursprungszugriffssteuerungen im Konto	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListOriginRequestPolicies	Gewährt die Berechtigung zum Auflisten aller Ursprungsanforderungsrichtlinien auf, die in CloudFront für dieses Konto erstellt wurden.	List			
ListPublicKeys	Gewährt die Berechtigung zum Auflisten aller öffentlichen Schlüssel, die CloudFront für dieses Konto hinzugefügt wurden.	Auflisten			
ListRateCards [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von CloudFront-Rate-Cards für das Konto	Auflisten			
ListRealtimeLogConfigs	Gewährt die Berechtigung zum Abrufen einer Liste von Echtzeit-Protokollkonfigurationen	Auflisten			
ListResponseHeadersPolicies	Gewährt die Berechtigung zum Auflisten aller Antwort-Header-Richtlinien, die in CloudFront für dieses Konto erstellt wurden	Auflisten			
ListSavingsPlans [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Savings Plans im Konto	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListStreamingDistributions	Gewährt die Berechtigung zum Auflisten Ihrer RTMP-Verteilungen	List			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine CloudFront-Ressource	Lesen	distribution		
ListUsages [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der CloudFront-Nutzung	Auflisten			
PublishFunction	Gewährt die Berechtigung zum Veröffentlichen einer CloudFront Funktion	Write	function*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer CloudFront-Ressource.	Markieren	distribution		
			streaming-distribution		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestFunction	Gewährt die Berechtigung zum Testen einer CloudFront Funktion	Write	function*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer CloudFront-Ressource	Markieren	distribution		
			streaming-distribution		
				aws:TagKeys	
UpdateCachePolicy	Gewährt die Berechtigung zum Aktualisieren einer Cacherichtlinie	Write	cache-policy*		
UpdateCloudFrontOriginAccessIdentity	Gewährt die Berechtigung zum Festlegen der Konfiguration einer CloudFront Ursprungszugriffsidentität	Schreiben	origin-access-identity*		
UpdateContinuousDeploymentPolicy	Gewährt die Berechtigung zum Aktualisieren einer Richtlinie für die kontinuierliche Bereitstellung	Schreiben	continuous-deployment-policy*		
UpdateDistribution	Gewährt die Berechtigung zum Aktualisieren einer Webverteilung	Write	distribution*		
UpdateFieldLevelEncryptionConfig	Gewährt die Berechtigung zum Aktualisieren der Verschlüsselungskonfiguration auf Feldeben	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateFieldLevelEncryptionProfile	Gewährt die Berechtigung zum Aktualisieren eines Verschlüsselungsprofils auf Feldebene	Write	field-level-encryption-profile*		
UpdateFunction	Gewährt die Berechtigung zum Aktualisieren einer CloudFront-Funktion	Write	function*		
UpdateKeyGroup	Gewährt die Berechtigung zum Aktualisieren einer Schlüsselgruppe.	Schreiben			
UpdateKeyValueStore	Gewährt die Berechtigung zum Aktualisieren eines CloudFront KeyValueStore	Schreiben	key-value-store*		
UpdateOriginAccessControl	Gewährt die Berechtigung zum Aktualisieren einer Ursprungszugriffssteuerung	Schreiben	origin-access-control*		
UpdateOriginRequestPolicy	Gewährt die Berechtigung zum Aktualisieren einer Ursprungsanforderungsrichtlinie	Write	origin-request-policy*		
UpdatePublicKey	Gewährt die Berechtigung zum Aktualisieren von Informationen über öffentliche Schlüssel	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateRealtimeLogConfig	Gewährt die Berechtigung zum Aktualisieren einer Echtzeit-Protokollkonfiguration	Schreiben	realtime-log-config*		
UpdateResponseHeadersPolicy	Gewährt die Berechtigung zum Aktualisieren einer Antwort-Header-Richtlinie	Schreiben	response-headers-policy*		
UpdateSavingsPlan [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren eines Savings Plan	Schreiben			
UpdateStreamingDistribution	Gewährt die Berechtigung zum Aktualisieren einer RTMP-Verteilung	Write	streaming-distribution*		

Von Amazon CloudFront definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
distribution	`arn:${Partition}:cloudfront::${Account}:distribution/${DistributionId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
streaming-distribution	arn:${Partition}:cloudfront::${Account}:streaming-distribution/${DistributionId}	aws:ResourceTag/${TagKey}
origin-access-identity	arn:${Partition}:cloudfront::${Account}:origin-access-identity/${Id}	
field-level-encryption-config	arn:${Partition}:cloudfront::${Account}:field-level-encryption-config/${Id}	
field-level-encryption-profile	arn:${Partition}:cloudfront::${Account}:field-level-encryption-profile/${Id}	
cache-policy	arn:${Partition}:cloudfront::${Account}:cache-policy/${Id}	
origin-request-policy	arn:${Partition}:cloudfront::${Account}:origin-request-policy/${Id}	
realtime-log-config	arn:${Partition}:cloudfront::${Account}:realtime-log-config/${Name}	
function	arn:${Partition}:cloudfront::${Account}:function/${Name}	
key-value-store	arn:${Partition}:cloudfront::${Account}:key-value-store/${Name}	
response-headers-policy	arn:${Partition}:cloudfront::${Account}:response-headers-policy/${Id}	
origin-access-control	arn:${Partition}:cloudfront::${Account}:origin-access-control/${Id}	

Ressourcentypen	ARN	Bedingungsschlüssel
continuous-deployment-policy	`arn:${Partition}:cloudfront::${Account}:continuous-deployment-policy/${Id}`	

Bedingungsschlüssel für Amazon CloudFront

Amazon CloudFront definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CloudFront Schlüsselwertspeicher

Amazon CloudFront Schlüsselwertspeicher (Servicepräfix: `cloudfront-keyvaluestore`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon CloudFront Schlüsselwertspeicher definierte Aktionen
- Von Amazon CloudFront Schlüsselwertspeicher definierte Ressourcentypen
- Bedingungsschlüssel für Amazon CloudFront Schlüsselwertspeicher

Von Amazon CloudFront Schlüsselwertspeicher definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteKey	Gewährt die Berechtigung zum Löschen des durch den Schlüssel angegebenen Schlüssel-Wert-Paars	Schreiben	key-value-store*		
DescribeKeyValueStore	Gewährt die Berechtigung zum Zurückgeben von Informationen zu Metadaten eines Schlüsselwertspeichers	Lesen	key-value-store*		
GetKey	Gewährt die Berechtigung, ein Schlüssel-Wert-Paar zurückzugeben	Lesen	key-value-store*		
ListKeys	Gewährt die Berechtigung, eine Liste von Schlüssel-Wert-Paaren zurückzugeben	Auflisten	key-value-store*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutKey	Gewährt die Berechtigung, ein neues Schlüssel-Wert-Paar zu erstellen oder den Wert eines vorhandenen Schlüssels zu ersetzen	Schreiben	key-value-store*		
UpdateKeys	Gewährt die Berechtigung zum Ablegen oder Löschen mehrerer Schlüssel-Wert-Paare aus einer einzelnen Alles-oder-Nichts-Operation	Schreiben	key-value-store*		

Von Amazon CloudFront Schlüsselwertspeicher definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
key-value-store	`arn:${Partition}:cloudfront::${Account}:key-value-store/${ResourceId}`	

Bedingungsschlüssel für Amazon CloudFront Schlüsselwertspeicher

CloudFront Schlüsselwertspeicher umfasst keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen

Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS CloudHSM

AWS CloudHSM (Servicepräfix: `cloudhsm`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS CloudHSM definierte Aktionen
- Von AWS CloudHSM definierte Ressourcentypen
- Bedingungsschlüssel für AWS CloudHSM

Von AWS CloudHSM definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie

den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddTagsToResource	Fügt der angegebenen AWS CloudHSM-Ressource einzelne oder mehrere Tags hinzu oder überschreibt sie	Markierung			
CopyBackupToRegion	Gewährt die Berechtigung zum Erstellen einer Kopie einer Sicherung in der angegebenen Region	Schreiben	backup*		cloudhsm:CopyBackupToRegion cloudhsm:TagResource

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					cloudhsm:UntagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCluster	Gewährt die Berechtigung zum Erstellen eines neuen AWS CloudHSM-Clusters	Schreiben	backup		cloudhsm:TagResource ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:RevokeSecurityGroupEgress iam:CreateServiceL

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					inkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHapg	Erstellt eine Partitionsgruppe mit hoher Verfügbarkeit	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateHsm	Gewährt die Berechtigung zum Erstellen eines neuen Hardwaresicherheitsmoduls (HSM) im angegebenen AWS CloudHSM-Cluster	Schreiben	cluster*		ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ec2:RevokeSecurityGroupEgress
CreateLunaClient	Erstellt einen HSM-Client	Schreiben			
DeleteBackup	Gewährt die Berechtigung zum Löschen des angegebenen Load Balancers.	Schreiben	backup*		
DeleteCluster	Gewährt die Berechtigung zum Löschen des angegebenen AWS CloudHSM-Clusters	Schreiben	cluster*		ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup
DeleteHapg	Löscht eine Partitionsgruppe mit hoher Verfügbarkeit	Schreiben			
DeleteHsm	Gewährt die Berechtigung zum Löschen des angegebenen HSM	Schreiben			ec2:DeleteNetworkInterface
DeleteLunaClient	Löscht einen Client	Schreiben			
DescribeBackups	Gewährt die Berechtigung zum Abrufen von Informationen zu Sicherungen von AWS CloudHSM-Clustern	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeClusters	Gewährt die Berechtigung zum Abrufen von Informationen über AWS CloudHSM-Cluster	Lesen			
DescribeHapg	Ruft Informationen zu einer Partitionsgruppe mit hoher Verfügbarkeit ab	Read			
DescribeHsm	Ruft Informationen zu einem HSM ab. Sie können das HSM über den ARN oder die Seriennummer identifizieren	Read			
DescribeLunaClient	Ruft Informationen zu einem HSM-Client ab	Read			
GetConfig	Ruft die Konfigurationsdaten ab, die zum Herstellen der Verbindung zu allen Partitionsgruppen mit hoher Verfügbarkeit, denen der Client zugeordnet ist, erforderlich sind	Lesen			
InitializeCluster	Gewährt die Berechtigung zur Beantragung eines AWS CloudHSM-Clusters	Schreiben	cluster*		
ListAvailableZones	Listet die Availability Zones auf, die über verfügbare AWS CloudHSM-Kapazität verfügen	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListHapgs	Listet die Partitionsgruppen mit hoher Verfügbarkeit für das Konto auf	List			
ListHsms	Ruft die Kennungen aller für den aktuellen Kunden bereitgestellten HSMs ab	List			
ListLunaClients	Listet alle Clients auf	Auflisten			
ListTags	Gewährt die Berechtigung zum Abrufen einer Aufgabenliste für das angegebene AWS CloudHSM-Cluster	Lesen	backup cluster		
ListTagsForResource	Gibt eine Liste aller Tags für die angegebene AWS CloudHSM-Ressource zurück	Lesen			
ModifyBackupAttributes	Gewährt die Berechtigung zum Ändern von Attributen für ein AWS CloudHSM-Backup	Schreiben	backup*		
ModifyCluster	Gewährt die Berechtigung zum Ändern des AWS CloudHSM-Clusters	Schreiben	cluster*		
ModifyHapg	Ändert eine Partitionsgruppe mit hoher Verfügbarkeit	Write			
ModifyHsm	Ändert ein HSM	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyLunaClient	Ändert das vom Client verwendete Zertifikat	Write			
RemoveTagsFromResource	Entfernt einzelne oder mehrere Tags aus der angegebenen AWS CloudHSM-Ressource	Markierung			
RestoreBackup	Gewährt die Berechtigung zum Wiederherstellen des angegebenen CloudHSM-Backups	Schreiben	backup*		
TagResource	Gewährt die Berechtigung zum Hinzufügen oder Überschreiben von einem oder mehreren Tags für das AWS CloudHSM-Cluster	Markierung	backup		
			cluster		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen des/der angegebenen Tags aus dem angegebenen AWS CloudHSM-Cluster	Markierung	backup		
			cluster		
				aws:TagKeys	

Von AWS CloudHSM definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
backup	`arn:${Partition}:cloudhsm:${Region}:${Account}:backup/${CloudHsmBackupInstanceName}`	aws:ResourceTag/${TagKey}
cluster	`arn:${Partition}:cloudhsm:${Region}:${Account}:cluster/${CloudHsmClusterInstanceName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS CloudHSM

AWS CloudHSM definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CloudSearch

Amazon CloudSearch (Servicepräfix: `cloudsearch`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon CloudSearch definierte Aktionen
- Von Amazon CloudSearch definierte Ressourcentypen
- Bedingungsschlüssel für Amazon CloudSearch

Von Amazon CloudSearch definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddTags	Fügt Ressourcen-Tags an eine Amazon CloudSearch-Domain an	Markierung	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BuildSuggesters	Indiziert die Suchvorschläge	Schreiben	domain*		
CreateDomain	Erstellt eine neue Such-Domain	Schreiben	domain*		
DefineAnalysisScheme	Konfiguriert ein Analyseschema, das zum Definieren sprachspezifischer Textverarbeitungsoptionen auf ein Text- oder Text-Array-Feld angewendet werden kann	Schreiben	domain*		
DefineExpression	Konfiguriert einen Ausdruck für die Such-Domain	Schreiben	domain*		
DefineIndexField	Konfiguriert ein IndexField für die Such-Domain	Schreiben	domain*		
DefineSuggester	Konfiguriert Vorschläge für eine Domain	Schreiben	domain*		
DeleteAnalysisScheme	Löscht ein Analyseschema	Schreiben	domain*		
DeleteDomain	Löscht eine Such-Domain und deren Daten endgültig	Schreiben	domain*		
DeleteExpression	Entfernt einen Ausdruck aus der Such-Domain	Schreiben	domain*		
DeleteIndexField	Entfernt ein IndexField aus der Such-Domain	Schreiben	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteSuggester	Löscht Vorschläge	Schreiben	domain*		
DescribeAnalysisSchemes	Ruft die für eine Domain konfigurierten Analyseschemas ab	Lesen	domain*		
DescribeAvailabilityOptions	Ruft die für eine Domain konfigurierten Verfügbarkeitsoptionen ab	Lesen	domain*		
DescribeDomainEndpointOptions	Ruft die Domain-Endpunktoptionen ab, die für eine Domain konfiguriert sind	Lesen	domain*		
DescribeDomains	Ruft Informationen zu den Suchdomains ab, die sich im Besitz dieses Kontos befinden	Auflisten	domain*		
DescribeExpressions	Ruft die für die Such-Domain konfigurierten Ausdrücke ab	Lesen	domain*		
DescribeIndexFields	Ruft Informationen zu den für die Such-Domain konfigurierten Indexfeldern ab	Lesen	domain*		
DescribeScalingParameters	Ruft die für eine Domain konfigurierten Skalierungsparameter ab	Lesen	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeServiceAccessPolicies	Ruft Informationen zu den Zugriffsrichtlinien ab, die den Zugriff auf die Dokument- und Suchendpunkte der Domain steuern	Lesen	domain*		
DescribeSuggesters	Ruft die für eine Domain konfigurierten Vorschläge ab	Lesen	domain*		
IndexDocuments	Weist die Such-Domain an, die Indizierung der Dokumente mit den neuesten Indizierungsoptionen zu starten	Schreiben	domain*		
ListDomainNames	Listet alle Suchdomains auf, die einem Konto gehören	Auflisten	domain*		
ListTags	Zeigt alle Ressourcen-Tags für eine Amazon-CloudSearch-Domain an	Lesen	domain*		
RemoveTags	Entfernt die angegebenen Ressourcen-Tags aus einer Amazon-ES-Domain	Markierung	domain*		
UpdateAvailabilityOptions	Konfiguriert die Verfügbarkeitsoptionen für eine Domain	Schreiben	domain*		
UpdateDomainEndpointOptions	Konfiguriert die Domain-Endpunkt-Optionen für eine Domain	Schreiben	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateScalingParameters	Konfiguriert die Skalierungsparameter für eine Domain	Schreiben	domain*		
UpdateServiceAccessPolicies	Konfiguriert die Zugriffsregeln, die den Zugriff auf die Dokument- und Suchendpunkte der Domain steuern	Berechtigungsverwaltung	domain*		
document [nur Berechtigung]	Ermöglicht den Zugriff auf die Dokument-Service-Vorgänge	Schreiben	domain		
search [nur Berechtigung]	Ermöglicht den Zugriff auf die Suchvorgänge	Lesen	domain		
suggest [nur Berechtigung]	Ermöglicht den Zugriff auf die Vorschlagsvorgänge	Lesen	domain		

Von Amazon CloudSearch definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types (Ressourcen-Typen).

> **Note**
>
> Weitere Informationen zur Verwendung von Amazon CloudSearch-Ressourcen-ARNs in einer IAM-Richtlinie finden Sie unter Amazon CloudSearch ARNs im Amazon CloudSearch-Entwicklerhandbuch.

Ressourcentypen	ARN	Bedingungsschlüssel
domain	`arn:${Partition}:cloudsearch:${Region}:${Account}:domain/${DomainName}`	

Bedingungsschlüssel für Amazon CloudSearch

CloudSearch besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS CloudShell

AWS CloudShell (Servicepräfix: `cloudshell`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS CloudShell definierte Aktionen
- Von AWS CloudShell definierte Ressourcentypen
- Bedingungsschlüssel für AWS CloudShell

Von AWS CloudShell definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateEnvironment [nur Berechtigung]	Gewährt Berechtigungen zum Erstellen einer CloudShell-Umgebung	Write			
CreateSession [nur Berechtigung]	Gewährt Berechtigungen zum Herstellen einer Verbindung mit einer CloudShell-Umgebung über die AWS Management Console	Write	Environment*		
DeleteEnvironment [nur Berechtigung]	Gewährt die Berechtigung zum Löschen einer CloudShell-Umgebung	Write	Environment*		
GetEnvironmentStatus [nur Berechtigung]	Gewährt die Berechtigung zum Lesen eines CloudShell-Umgebungsstatus	Read	Environment*		
GetFileDownloadUrls [nur Berechtigung]	Gewährt Berechtigungen zum Download von Dateien aus einer CloudShell-Umgebung	Write	Environment*		
GetFileUploadUrls [nur Berechtigung]	Gewährt Berechtigungen zum Upload von Dateien in eine CloudShell-Umgebung	Write	Environment*		
PutCredentials [nur Berechtigung]	Gewährt Berechtigungen zum Weiterleiten von Konsolen-Anmeldeinformationen an die Umgebung	Write	Environment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartEnvironment [nur Berechtigung]	Gewährt die Berechtigung zum Starten einer angehaltenen CloudShell-Umgebung	Write	Environment*		
StopEnvironment [nur Berechtigung]	Gewährt die Berechtigung zum Stoppen einer laufenden CloudShell-Umgebung	Write	Environment*		

Von AWS CloudShell definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Environment	`arn:${Partition}:cloudshell:${Region}:${Account}:environment/${EnvironmentId}`	

Bedingungsschlüssel für AWS CloudShell

CloudShell hat keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS CloudTrail

AWS CloudTrail (Servicepräfix: `cloudtrail`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS CloudTrail definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddTags	Gewährt die Berechtigung zum Hinzufügen von einem oder mehreren Tags zu einem Trail, Ereignisdatenspeicher oder Kanal (maximal 50)	Tagging	channel		
			eventdatastore		
			trail		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelQuery	Gewährt die Berechtigung zum Abbrechen einer laufenden Abfrage	Schreiben	eventdatastore*		
CreateChannel	Gewährt die Berechtigung zum Erstellen eines Channels.	Schreiben	channel*		cloudtrail:AddTags
			eventdatastore*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateEventDataStore	Gewährt die Berechtigung zum Erstellen eines Ereignisdatenspeichers	Schreiben	eventdatastore*		cloudtrail:AddTags iam:CreateServiceLinkedRole iam:GetRole kms:Decrypt kms:GenerateDataKey organizations:ListAWSServiceAccessForOrganization
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateServiceLinkedChannel [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines serviceverknüpften Kanals, der die Einstellungen für die Bereitstellung von Protokolldaten an einen - AWS Service angibt	Schreiben	channel*		
CreateTrail	Gewährt die Berechtigung zum Erstellen eines Trails, der die Einstellungen für die Übermittlung von Protokolldaten an einen Amazon-S3-Bucket angibt	Schreiben	trail*		cloudtrail:AddTags iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Gewährt die Berechtigung zum Löschen eines Channels.	Schreiben	channel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteEventDataStore	Gewährt die Berechtigung zum Löschen eines Ereignisdatenspeichers	Schreiben	eventdatastore*		
DeleteResourcePolicy	Gewährt die Berechtigung zum Löschen einer Ressourcenrichtlinie aus der bereitgestellten Ressource	Schreiben	channel*		
DeleteServiceLinkedChannel [nur Berechtigung]	Gewährt die Berechtigung zum Löschen eines serviceverknüpften Kanals	Schreiben	channel*		
DeleteTrail	Gewährt die Berechtigung zum Löschen eines Trails	Schreiben	trail*		
DeregisterOrganizationDelegatedAdmin	Gewährt die Berechtigung zum Aufheben der Registrierung eines AWS -Organizations-Mitgliedskontos als delegierter Administrator	Schreiben			organizations:DeregisterDelegatedAdministrator organizations:ListAWSServiceAccessForOrganization

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeQuery	Gewährt die Berechtigung zum Auflisten von Details für die Abfrage	Lesen	eventdatastore*		
DescribeTrails	Gewährt die Berechtigung zum Auflisten von Einstellungen für die Trails, die mit der aktuellen Region für Ihr Konto verknüpft sind	Lesen			
DisableFederation	Gewährt die Berechtigung zum Deaktivieren des Verbunds von Ereignisdatenspeicherdaten mithilfe des AWS Glue Data Catalog	Schreiben	eventdatastore*		glue:DeleteDatabase glue:DeleteTable glue:PassConnection lakeformation:DeregisterResource lakeformation:RegisterResource

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
EnableFederation	Gewährt die Berechtigung zum Aktivieren des Verbunds von Ereignisdatenspeicherdaten mithilfe des AWS Glue Data Catalog	Schreiben	eventdatastore*		glue:CreateDatabase glue:CreateTable iam:GetRole iam:PassRole lakeformation:DeregisterResource lakeformation:RegisterResource
GetChannel	Gewährt die Berechtigung zum Abrufen von Informationen zu einem bestimmten Kanal	Lesen	channel*		
GetEventDataStore	Gewährt die Berechtigung zum Auflisten von Einstellungen für den Ereignisdatenspeicher	Lesen	eventdatastore*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetEventDataStoreData	Gewährt die Berechtigung zum Abrufen von Daten aus einem Ereignisdatenspeicher mithilfe des AWS Glue Data Catalog	Lesen	eventdatastore*		kms:Decrypt kms:GenerateDataKey
GetEventSelectors	Gewährt die Berechtigung zum Auflisten von Einstellungen für Ereignisauswahlen, die für einen Trail konfiguriert sind	Lesen	trail*		
GetImport	Gewährt die Berechtigung zum Zurückgeben von Informationen über einen spezifischen Import	Lesen			
GetInsightSelectors	Gewährt die Berechtigung zum Auflisten von CloudTrail Insights-Selektoren, die für einen Trail oder Ereignisdatenspeicher konfiguriert sind	Lesen	eventdatastore		
			trail		
GetQueryResults	Gewährt die Berechtigung zum Abrufen des Ergebnisses einer vollständigen Abfrage	Lesen	eventdatastore*		kms:Decrypt kms:GenerateDataKey

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetResourcePolicy	Gewährt die Berechtigung zum Abrufen der Ressourcenrichtlinie, die an eine bereitgestellte Ressource angefügt ist	Lesen	channel*		
GetServiceLinkedChannel [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Einstellungen für den serviceverknüpften Kanal	Lesen	channel*		
GetTrail	Gewährt die Berechtigung zum Auflisten von Einstellungen für den Trail	Read	trail*		
GetTrailStatus	Gewährt die Berechtigung zum Abrufen einer JSON-formatierten Liste von Informationen zum angegebenen Trail	Lesen	trail*		
ListChannels	Gewährt die Berechtigung zum Auflisten der Kanäle im aktuellen Konto und deren Quellnamen	Auflisten			
ListEventDataStores	Gewährt die Berechtigung zum Auflisten von Ereignisdatenspeichern, die der aktuellen Region für Ihr Konto zugeordnet sind	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListImportFailures	Gewährt die Berechtigung zum Zurückgeben einer Liste von Fehlern für den angegebenen Import	Lesen			
ListImports	Gewährt die Berechtigung zum Zurückgeben von Informationen zu allen Importen oder einem ausgewählten Satz von Importen nach ImportStatus oder Ziel	Auflisten			
ListPublicKeys	Gewährt die Berechtigung zum Auflisten der öffentlichen Schlüssel, deren private Schlüssel innerhalb eines angegebenen Zeitraums zum Signieren der Trail-Digest-Dateien verwendet wurden	Lesen			
ListQueries	Gewährt die Berechtigung zum Auflisten von Abfragen, die einem Ereignisdatenspeicher zugeordnet sind	Auflisten	eventdatastore*		
ListServiceLinkedChannels [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von serviceverknüpften Kanälen, die der aktuellen Region für ein angegebenes Konto zugeordnet sind	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTags	Gewährt die Berechtigung zum Auflisten der Tags für Trails, Ereignisdatenspeicher oder Kanäle in der aktuellen Region	Lesen	channel		
			eventdatastore		
			trail		
ListTrails	Gewährt die Berechtigung zum Auflisten von Trails, die mit der aktuellen Region für Ihr Konto verknüpft sind	Auflisten			
LookupEvents	Gewährt die Berechtigung zum Suchen und Abrufen von Metrikdaten für API-Aktivitätsereignisse, CloudTrail die von erfasst werden und Ressourcen in Ihrem Konto erstellen, aktualisieren oder löschen	Lesen			
PutEventSelectors	Gewährt die Berechtigung zum Erstellen und Aktualisieren von Ereignisauswahlen für einen Trail	Schreiben	trail*		
PutInsightSelectors	Gewährt die Berechtigung zum Erstellen und Aktualisieren von CloudTrail Insights-Selektoren für einen Trail oder Ereignisdatenspeicher	Schreiben	eventdatastore		
			trail		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutResourcePolicy	Gewährt die Berechtigung zum Anfügen einer Ressourcenrichtlinie an die bereitgestellte Ressource	Schreiben	channel*		
RegisterOrganizationDelegatedAdmin	Gewährt die Berechtigung zum Registrieren eines - AWS Organizations-Mitgliedskontos als delegierter Administrator	Schreiben			iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization organizations:RegisterDelegatedAdministrator
RemoveTags	Gewährt die Berechtigung zum Entfernen von Tags von einem Trail, einem Ereignisdatenspeicher oder Kanal	Tagging	channel		
			eventdatastore		
			trail		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RestoreEventDataStore	Gewährt die Berechtigung zum Wiederherstellen eines Ereignisdatenspeichers	Schreiben	eventdatastore*		
StartEventDataStoreIngestion	Gewährt die Berechtigung zum Starten der Aufnahme in einen Ereignisdatenspeicher	Schreiben	eventdatastore*		
StartImport	Gewährt die Berechtigung zum Starten eines Imports protokollierter Trail-Ereignisse aus einem S3-Quell-Bucket in einen Zielereignisdatenspeicher	Schreiben			
StartLogging	Gewährt die Berechtigung zum Starten der Aufzeichnung von AWS API-Aufrufen und der Bereitstellung von Protokolldateien für einen Trail	Schreiben	trail*		
StartQuery	Gewährt die Berechtigung zum Starten einer neuen Abfrage für einen bestimmten Ereignisdatenspeicher	Schreiben	eventdatastore*		kms:Decrypt kms:GenerateDataKey
StopEventDataStoreIngestion	Gewährt die Berechtigung zum Stoppen der Aufnahme in einen Ereignisdatenspeicher	Schreiben	eventdatastore*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopImport	Gewährt die Berechtigung zum Anhalten eines angegebenen Imports	Schreiben			
StopLogging	Gewährt die Berechtigung zum Stoppen der Aufzeichnung von AWS API-Aufrufen und der Bereitstellung von Protokolldateien für einen Trail	Schreiben	trail*		
UpdateChannel	Gewährt die Berechtigung zum Aktualisieren eines Channels.	Schreiben	channel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateEventDataStore	Gewährt die Berechtigung zum Aktualisieren eines Ereignisdatenspeichers	Schreiben	eventdatastore*		iam:CreateServiceLinkedRole iam:GetRole kms:Decrypt kms:GenerateDataKey organizations:ListAWSServiceAccessForOrganization
UpdateServiceLinkedChannel [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren die Einstellungen zur Übermittlung von Protokolldateien	Schreiben	channel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateTrail	Gewährt die Berechtigung zum Aktualisieren die Einstellungen zur Übermittlung von Protokolldateien	Schreiben	trail*		iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization

Von AWS CloudTrail definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

> **Note**
>
> Bei Richtlinien, die den Zugriff auf - CloudTrail Aktionen steuern, ist das Ressourcenelement immer auf „*“ gesetzt. Informationen zur Verwendung von Ressourcen-ARNs in einer IAM-Richtlinie finden Sie unter So AWS CloudTrail funktioniert mit IAM im AWS CloudTrail - Benutzerhandbuch.

Ressourcentypen	ARN	Bedingungsschlüssel
trail	`arn:${Partition}:cloudtrail:${Region}:${Account}:trail/${TrailName}`	
eventdatastore	`arn:${Partition}:cloudtrail:${Region}:${Account}:eventdatastore/${EventDataStoreId}`	aws:ResourceTag/${TagKey}
channel	`arn:${Partition}:cloudtrail:${Region}:${Account}:channel/${ChannelId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS CloudTrail

AWS CloudTrail definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tag-Schlüssel-Wert-Paare in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff über die Tags, die an die Ressource angehängt sind.	String
aws:TagKeys	Filtert den Zugriff nach den Tag-Schlüsseln in einer Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS-CloudTrail-Daten

AWS-CloudTrail-Daten (Servicepräfix: `cloudtrail-data`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS-CloudTrail-Daten definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutAuditEvents	Gewährt die Berechtigung zum Erfassen Ihrer Anwendungsereignisse in CloudTrail Lake	Schreiben	channel*		

Von AWS-CloudTrail-Daten definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen

angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types (Ressourcen-Typen).

> **Note**
>
> In Richtlinien, die den Zugriff auf CloudTrail-Aktionen steuern, hat das Element „Resource“ immer den Wert „*“. Informationen zur Verwendung von Ressourcen-ARNs in einer IAM-Richtlinie finden Sie unter So funktionieren AWS CloudTrail mit IAM im AWS CloudTrail-Benutzerhandbuch.

Ressourcentypen	ARN	Bedingungsschlüssel
channel	`arn:${Partition}:cloudtrail:${Region}:${Account}:channel/${ChannelId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS-CloudTrail-Daten

AWS-CloudTrail-Daten definieren die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Schlüssel eines Tags und den Wert einer Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung.	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert den Zugriff nach den Tag-Schlüsseln in einer Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CloudWatch

Amazon CloudWatch (Servicepräfix: `cloudwatch`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon CloudWatch definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn

die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetServiceLevelIndicatorReport	Gewährt die Berechtigung zum Batch-Abruf eines Service-Level-Indicator-Berichts	Lesen			
BatchGetServiceLevelObjecti	Gewährt die Berechtigung zum Batch-Abruf eines	Lesen	slo*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
veBudgetReport	Service-Level-Ziel-Budgetberichts				
CreateServiceLevelObjective	Gewährt die Berechtigung zum Erstellen eines Service-Level-Ziels	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAlarms	Gewährt die Berechtigung zum Löschen einer Sammlung von Alarmen	Write	alarm*		
DeleteAnomalyDetector	Gewährt die Berechtigung zum Löschen des angegebenen Anomalieerkennungsmodells aus Ihrem Konto	Write			
DeleteDashboards	Gewährt die Berechtigung zum Löschen aller von Ihnen angegebenen CloudWatch-Dashboards	Write	dashboard*		
DeleteInsightRules	Gewährt die Berechtigung zum Löschen einer Sammlung von Einsichtsregeln	Write	insight-rule*		
DeleteMetricStream	Gewährt die Berechtigung zum Löschen des von Ihnen angegebenen CloudWatch Metric Streams	Schreiben	metric-stream*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteServiceLevelObjective	Gewährt die Berechtigung zum Löschen eines Service-Level-Ziels	Schreiben	slo*		
DescribeAlarmHistory	Gewährt die Berechtigung zum Abrufen des Verlaufs für den angegebenen Alarm	Read	alarm*		
DescribeAlarms	Gewährt die Berechtigung zum Beschreiben aller Alarme, die derzeit im Besitz des Benutzerkontos sind.	Read	alarm*		
DescribeAlarmsForMetric	Gewährt die Berechtigung zum Beschreiben aller Alarme, die für die angegebene Metrik konfiguriert sind, die derzeit im Besitz des Benutzerkontos ist	Read			
DescribeAnomalyDetectors	Gewährt die Berechtigung zum Auflisten der Anomalieerkennungsmodelle, die Sie in Ihrem Konto erstellt haben	Read			
DescribeInsightRules	Gewährt die Berechtigung zum Beschreiben alle Einsichtsregeln, die derzeit im Besitz des Benutzerkontos sind	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisableAlarmActions	Gewährt die Berechtigung zum Deaktivieren von Aktionen für eine Sammlung von Alarmen	Write	alarm*		
DisableInsightRules	Gewährt die Berechtigung zum Deaktivieren einer Sammlung von Einsichtsregeln	Write	insight-rule*		
EnableAlarmActions	Gewährt die Berechtigung zum Aktivieren von Aktionen für eine Sammlung von Alarmen	Write	alarm*		
EnableInsightRules	Gewährt die Berechtigung zum Aktivieren einer Sammlung von Einsichtsregeln	Schreiben	insight-rule*		
EnableTopologyDiscovery	Gewährt die Berechtigung zum Aktivieren einer CloudWatch-Topologieerkennung	Schreiben			
GenerateQuery	Gewährt die Berechtigung, anhand einer Aufforderung in natürlicher Sprache eine Metrics Insights- oder Logs Insights-Abfragezeichenfolge zu generieren	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDashboard	Gewährt die Berechtigung zum Anzeigen der Details des von Ihnen angegebenen CloudWatch-Dashboards	Read	dashboard*		
GetInsightRuleReport	Gewährt die Berechtigung für das Zurückgeben der Top-N-Berichte der eindeutigen Beitragenden über einen Zeitraum für eine bestimmte Einsichtsregel	Read	insight-rule*		
GetMetricData	Gewährt die Berechtigung zum Batchabruf von CloudWatch-Kennzahlen und zum Ausführen von Metrikberechnungen für die abgerufenen Daten	Read			
GetMetricStatistics	Gewährt die Berechtigung zum Abrufen von Statistiken für die angegebene Metrik	Read			
GetMetricStream	Gewährt die Berechtigung, die Details eines CloudWatch Metric Streams zurückzugeben	Read	metric-stream*		
GetMetricWidgetImage	Gewährt die Berechtigung zum Abrufen von Snapshots von Metrik-Widgets	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetService	Gewährt die Berechtigung zum Abrufen von Informationen über einen Service	Lesen	service*		
GetServiceData [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Servicedaten	Lesen	service*		
GetServiceLevelObjective	Gewährt die Berechtigung zum Abrufen von Informationen zum Servicelevel-Ziel	Lesen	slo*		
GetTopologyDiscoveryStatus [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen eines CloudWatch-Topologie-Discovery-Status	Lesen			
GetTopologyMap	Gewährt die Berechtigung zum Abrufen einer CloudWatch-Topologiemap	Lesen			
Link [nur Berechtigung]	Gewährt die Berechtigung zum Freigeben von CloudWatch-Ressourcen für ein Überwachungs-Konto	Schreiben			
ListDashboards	Gewährt die Berechtigung zum Zurückgeben einer Liste aller CloudWatch-Dashboards in Ihrem Konto	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListManagedInsightRules	Gewährt die Berechtigung zum Auflisten der verfügbaren verwalteten Insight-Regeln für einen bestimmten Ressourcen-ARN.	Lesen		aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestManagedResourceARNs	
ListMetricStreams	Gewährt die Berechtigung zum Zurückgeben einer Liste aller CloudWatch Metric Streams in Ihrem Konto	List			
ListMetrics	Gewährt die Berechtigung zum Abrufen einer Liste gültiger Metriken, die für den Besitzer des AWS-Konto gespeichert sind	Auflisten			
ListServiceLevelObjectives	Gewährt die Berechtigung zum Auflisten von Service-Level-Zielen	Auflisten			
ListServices	Gewährt die Berechtigung zum Auflisten von Services	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Amazon-CloudWatch-Ressource	List	alarm		
			insight-rule		
			slo		
	SZENARIO: CloudWatch-Alarm		alarm*		
	SZENARIO: CloudWatch-InsightRule		insight-rule*		
	SZENARIO: CloudWatch-ServiceLevelObjective		slo*		
PutAnomalyDetector	Gewährt die Berechtigung zum Erstellen oder Aktualisieren eines Anomaliedetektionsmodells für eine CloudWatch-Metrik	Write			
PutCompositeAlarm	Gewährt die Berechtigung zum Erstellen oder Aktualisieren eines zusammengesetzten Alarms	Write	alarm*		
				aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:AlarmActions	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutDashboard	Gewährt die Berechtigung zum Erstellen eines CloudWatch-Dashboards oder zum Aktualisieren eines vorhandenen Dashboards, falls es bereits vorhanden ist	Write	dashboard*		
PutInsightRule	Gewährt die Berechtigung zum Erteilen einer neuen oder zum Ersetzen einer vorhanden Einsichtsregel	Schreiben	insight-rule*		
				aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestInsightRuleLogGroups	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutManagedInsightRules	Gewährt die Berechtigung zum Erstellen verwalteter Insight-Regeln.	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestManagedResourceARNs	
PutMetricAlarm	Gewährt die Berechtigung zum Erstellen oder Aktualisieren eines Alarms und ordnet ihn der angegebenen Amazon-CloudWatch-Metrik zu	Write	alarm*	aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:AlarmActions	
PutMetricData	Gewährt die Berechtigung zum Veröffentlichen von Metrikdatenpunkten in Amazon CloudWatch	Write		cloudwatch:namespace	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutMetricStream	Gewährt die Berechtigung, einen CloudWatch Metric Stream zu erstellen oder einen vorhandenen Metric Stream zu aktualisieren, falls er bereits vorhanden ist	Write	metric-stream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
SetAlarmState	Gewährt die Berechtigung zum vorübergehen Festlegen des Status eines Alarms für Testzwecke	Write	alarm*		
StartMetricStreams	Gewährt die Berechtigung, alle von Ihnen angegebenen CloudWatch Metric Streams zu starten	Write	metric-stream*		
StopMetricStreams	Gewährt die Berechtigung, alle von Ihnen angegebenen CloudWatch Metric Streams zu stoppen	Write	metric-stream*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Amazon-CloudWatch-Ressource	Markieren	alarm		
			insight-rule		
			slo		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
	SZENARIO: CloudWatch-Alarm		alarm*		
	SZENARIO: CloudWatch-InsightRule		insight-rule*		
	SZENARIO: CloudWatch-ServiceLevelObjective		slo*		
UntagResource	Gewährt die Berechtigung zum Entfernen eines Tags aus einer Amazon-CloudWatch-Ressource	Markieren	alarm		
			insight-rule		
			slo		
				aws:TagKeys	
	SZENARIO: CloudWatch-Alarm		alarm*		
	SZENARIO: CloudWatch-InsightRule		insight-rule*		
	SZENARIO: CloudWatch-ServiceLevelObjective		slo*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateServiceLevelObjective	Gewährt die Berechtigung zum Aktualisieren eines Service-Level-Ziels	Schreiben	slo*		

Von Amazon CloudWatch definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
alarm	`arn:${Partition}:cloudwatch:${Region}:${Account}:alarm:${AlarmName}`	aws:ResourceTag/${TagKey}
dashboard	`arn:${Partition}:cloudwatch::${Account}:dashboard/${DashboardName}`	
insight-rule	`arn:${Partition}:cloudwatch:${Region}:${Account}:insight-rule/${InsightRuleName}`	aws:ResourceTag/${TagKey}
metric-stream	`arn:${Partition}:cloudwatch:${Region}:${Account}:metric-stream/${MetricStreamName}`	aws:ResourceTag/${TagKey}
slo	`arn:${Partition}:cloudwatch:${Region}:${Account}:slo/${SloName}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
service	`arn:${Partition}:cloudwatch:${Region}:${Account}:service/${ServiceName}-${UniqueAttributesHex}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon CloudWatch

Amazon CloudWatch definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf den zulässigen Werten für die einzelnen Tags	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf dem Tag-Wert, der der Ressource zugeordnet ist.	Zeichenfolge
aws:TagKeys	Filtert Aktionen basierend auf den obligatorischen Tags in der Anforderung	ArrayOfString
cloudwatch:AlarmActions	Filtert Aktionen basierend auf definierten Alarmaktionen	ArrayOfString
cloudwatch:namespace	Filtert Aktionen basierend auf optionalen Namespace-Werten.	Zeichenfolge
cloudwatch:request	Filtert Aktionen basierend auf den in einer Insight-Regel angegebenen Protokollgruppen	ArrayOfString

Bedingungsschlüssel	Beschreibung	Typ
InsightRuleLogGroups		
cloudwatch:requestManagedResourceARNs	Filtert den Zugriff nach den in einer verwalteten Insight-Regel angegebenen Ressourcen-ARNs.	ArrayOfARN

Aktionen, Ressourcen und Zustandsschlüssel für Amazon CloudWatch Application Insights

Amazon CloudWatch Application Insights (Service-Präfix: `applicationinsights`) bietet die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon CloudWatch Application Insights definierte Aktionen
- Von Amazon CloudWatch Application Insights definierte Ressourcentypen
- Zustandsschlüssel für Amazon CloudWatch Application Insights

Von Amazon CloudWatch Application Insights definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddWorkload	Erteilt die Berechtigung zum Hinzufügen einer Workload	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateApplication	Gewährt die Berechtigung zum Erstellen einer Anwendung aus einer Ressourcengruppe	Write			
CreateComponent	Gewährt die Berechtigung zum Erstellen einer Komponente aus einer Gruppe von Ressourcen	Write			
CreateLogPattern	Gewährt die Berechtigung zum Erstellen eines Protokollmusters	Write			
DeleteApplication	Gewährt die Berechtigung zum Löschen einer Anwendung	Write			
DeleteComponent	Gewährt die Berechtigung zum Löschen einer Komponente	Write			
DeleteLogPattern	Gewährt die Berechtigung zum Löschen eines Protokollmusters	Write			
DescribeApplication	Gewährt die Berechtigung zum Beschreiben einer Anwendung	Read			
DescribeComponent	Gewährt die Berechtigung zum Beschreiben eines Kontakts	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeComponentConfiguration	Gewährt die Berechtigung, die Konfiguration einer Komponente zu beschreiben	Read			
DescribeComponentConfigurationRecommendation	Gewährt die Berechtigung, die empfohlene Konfiguration der Anwendungskomponenten zu beschreiben	Read			
DescribeLogPattern	Gewährt die Berechtigung zum Beschreiben eines Protokollmusters	Read			
DescribeObservation	Gewährt die Berechtigung zum Beschreiben einer Beobachtung	Read			
DescribeProblem	Gewährt die Berechtigung zum Beschreiben eines Problems	Read			
DescribeProblemObservations	Gewährt die Berechtigung zum Beschreiben der Beobachtung in einem Problem	Lesen			
DescribeWorkload	Erteilt die Berechtigung zum Beschreiben einer Workload	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Link [nur Berechtigung]	Gewährt die Berechtigung zum Freigeben von Application-Insights-Ressourcen für ein Überwachungskonto	Schreiben			
ListApplications	Gewährt die Berechtigung zum Auflisten aller Anwendungen	List			
ListComponents	Gewährt die Berechtigung zum Auflisten der Komponenten einer Anwendung	List			
ListConfigurationHistory	Gewährt die Berechtigung zum Auflisten des Konfigurationsverlaufs	List			
ListLogPatternSets	Gewährt die Berechtigung zum Auflisten von Protokollmustersätzen für eine Anwendung	List			
ListLogPatterns	Gewährt die Berechtigung zum Auflisten von Protokollmustern	List			
ListProblems	Gewährt die Berechtigung zum Auflisten der Probleme in einer Anwendung	List			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListWorkloads	Gewährt die Berechtigung zum Auflisten von Workloads	Auflisten			
RemoveWorkload	Erteilt die Berechtigung zum Entfernen einer Workload	Schreiben			
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren		aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Markieren		aws:TagKeys	
UpdateApplication	Gewährt die Berechtigung zum Aktualisieren einer Anwendung	Write			
UpdateComponent	Gewährt die Berechtigung zum Aktualisieren einer Komponente	Write			
UpdateComponentConfiguration	Gewährt die Berechtigung zum Aktualisieren der Konfiguration einer Komponente	Write			
UpdateLogPattern	Gewährt die Berechtigung zum Aktualisieren eines Protokollmusters	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateProblem	Erteilt die Berechtigung zum Aktualisieren eines Problems	Schreiben			
UpdateWorkload	Erteilt die Berechtigung zum Aktualisieren einer Workload	Schreiben			

Von Amazon CloudWatch Application Insights definierte Ressourcentypen

Amazon CloudWatch Application Insights unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource` Element einer IAM-Richtlinie. Um den Zugriff auf Amazon CloudWatch Application Insights zu ermöglichen, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Zustandsschlüssel für Amazon CloudWatch Application Insights

Amazon CloudWatch Application Insights definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wertepaaren, die in der Anforderung zulässig sind	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paar einer Ressource	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert den Zugriff nach Liste von Tag-Schlüsseln, die in der Anforderung zulässig sind	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CloudWatch Evidently

Amazon CloudWatch Evidently (Servicepräfix: `evidently`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon CloudWatch Evidently definierte Aktionen
- Von Amazon CloudWatch Evidently definierte Ressourcentypen
- Bedingungsschlüssel für Amazon CloudWatch Evidently

Von Amazon CloudWatch Evidently definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchEvaluateFeature	Erteilt die Berechtigung zum Senden einer batchfähigen Evaluierungsfunktionsanforderung	Schreiben	Feature*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateExperiment	Gewährt die Berechtigung zum Erstellen eines Experiments	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFeature	Gewährt die Berechtigung zum Erstellen einer Funktion	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLaunch	Gewährt die Berechtigung zum Erstellen eines Starts	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProject	Gewährt die Berechtigung zum Erstellen eines Projekts	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole iam:GetRole
CreateSegment	Gewährt die Berechtigung zum Erstellen eines Segments	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteExperiment	Gewährt die Berechtigung zum Ausführen eines Experiments	Schreiben	Experiment*		
DeleteFeature	Gewährt die Berechtigung zum Löschen einer Funktion	Schreiben	Feature*		
DeleteLaunch	Gewährt die Berechtigung zum Löschen eines Starts	Schreiben	Launch*		
DeleteProject	Gewährt die Berechtigung zum Löschen eines Projekts	Schreiben	Project*		
DeleteSegment	Gewährt die Berechtigung zum Löschen eines Segments	Schreiben	Segment*		
EvaluateFeature	Erteilt die Berechtigung zum Senden einer Evaluierungsfunktionsanforderung	Schreiben	Feature*		
GetExperiment	Gewährt die Berechtigung zum Abrufen von Experimentdetails	Lesen	Experiment*		
GetExperimentResults	Gewährt die Berechtigung zum Abrufen des Experiment-Ergebnisses	Lesen	Experiment*		
GetFeature	Gewährt die Berechtigung zum Abrufen von Funktionsdetails	Lesen	Feature*		
GetLaunch	Gewährt die Berechtigung zum Abrufen von Startdetails	Lesen	Launch*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetProject	Gewährt die Berechtigung zum Abrufen von Projektdetails	Lesen	Project*		
GetSegment	Gewährt die Berechtigung zum Abrufen von Segmentdetails	Lesen	Segment*		
ListExperiments	Gewährt die Berechtigung, alle Experimente aufzulisten	Lesen			
ListFeatures	Gewährt die Berechtigung zum Auflisten von Funktionen	Lesen			
ListLaunches	Gewährt die Berechtigung zum Auflisten von Starts	Lesen			
ListProjects	Gewährt die Berechtigung zum Auflisten von Projekten	Lesen			
ListSegmentReferences	Gewährt die Berechtigung zum Auflisten von Ressourcen, die auf ein Segment verweisen	Lesen			
ListSegments	Gewährt die Berechtigung, Segmente aufzulisten	Lesen			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für Ressourcen	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutProjectEvents	Gewährt die Berechtigung zum Senden von Leistungsereignissen	Schreiben	Project*		
StartExperiment	Gewährt die Berechtigung zum Starten eines Experiments	Schreiben	Experiment*		
StartLaunch	Gewährt die Berechtigung zum Starten eines Launches	Schreiben	Launch*		
StopExperiment	Gewährt die Berechtigung zum Beenden eines Experiments	Schreiben	Experiment*		
StopLaunch	Gewährt die Berechtigung zum Beenden eines Launches	Schreiben	Launch*		
TagResource	Gewährt die Berechtigung zum Markieren von Ressourcen	Markierung	Experiment		
			Feature		
			Launch		
			Project		
			Segment		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
TestSegmentPattern	Gewährt die Berechtigung zum Testen eines Segmentmusters	Lesen			
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung von Ressourcen	Markierung	Experiment		
			Feature		
			Launch		
			Project		
			Segment		
				aws:TagKeys	
UpdateExperiment	Gewährt die Berechtigung zum Aktualisieren eines Experiments	Schreiben	Experiment*		
UpdateFeature	Gewährt die Berechtigung zum Aktualisieren einer Funktion	Schreiben	Feature*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateLaunch	Gewährt die Berechtigung zum Aktualisieren eines Launches	Schreiben	Launch*		
UpdateProject	Gewährt die Berechtigung zum Aktualisieren eines Projekts	Schreiben	Project*		iam:CreateServiceLinkedRole iam:GetRole
UpdateProjectDataDelivery	Gewährt die Berechtigung zum Aktualisieren der Bereitstellung von Projektdaten	Schreiben	Project*		

Von Amazon CloudWatch Evidently definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Project	`arn:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
Feature	`arn:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}/feature/${FeatureName}`	aws:ResourceTag/${TagKey}
Experiment	`arn:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}/experiment/${ExperimentName}`	aws:ResourceTag/${TagKey}
Launch	`arn:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}/launch/${LaunchName}`	aws:ResourceTag/${TagKey}
Segment	`arn:${Partition}:evidently:${Region}:${Account}:segment/${SegmentName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon CloudWatch Evidently

Amazon CloudWatch Evidently definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach den Tags, die von der Anforderung im Auftrag des IAM-Prinzipals weitergeleitet werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach den Tags, die der Ressource zugeordnet sind, die die Anforderung im Auftrag des IAM-Prinzipals tätigen	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert den Zugriff nach den Tag-Schlüsseln, die von der Anforderung im Auftrag des IAM-Prinzipals weitergeleitet werden	ArrayOfString

Aktionen, Ressourcen und Zustandstasten für Amazon CloudWatch Internet Monitor

Amazon CloudWatch Internet Monitor (Servicepräfix:`internetmonitor`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon CloudWatch Internet Monitor definierte Aktionen
- Von Amazon CloudWatch Internet Monitor definierte Ressourcentypen
- Zustandstasten für Amazon CloudWatch Internet Monitor

Von Amazon CloudWatch Internet Monitor definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateMonitor	Gewährt die Berechtigung zum Erstellen eines Monitors	Schreiben	Monitor*		
				aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
DeleteMonitor	Gewährt die Berechtigung zum Löschen eines Monitors	Schreiben	Monitor*		
GetHealthEvent	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Zustandsereignis für einen angegebenen Monitor	Lesen	HealthEvent*		
GetInternetEvent	Erteilt die Erlaubnis, Informationen über ein bestimmtes Internetereignis abzurufen	Lesen	InternetEvent*		
GetMonitor	Gewährt die Berechtigung zum Abrufen von Informationen über einen Monitor	Lesen	Monitor*		
GetQueryResults	Gewährt die Berechtigung zum Abrufen von Ergebnissen für eine Datenabfrage für einen Monitor	Lesen	Monitor*		
GetQueryStatus	Gewährt die Berechtigung zum Abrufen des Status für eine Datenabfrage für einen Monitor	Lesen	Monitor*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Link [nur Berechtigung]	Erteilt die Berechtigung, Internet Monitor-Ressourcen mit einem Überwachungskonto gemeinsam zu nutzen	Schreiben			
ListHealthEvents	Gewährt die Berechtigung zum Auflisten aller Zustandsereignisse für einen Monitor	Auflisten	Monitor*		
ListInternetEvents	Erteilt die Berechtigung, alle Internetereignisse aufzulisten	Auflisten			
ListMonitors	Gewährt die Berechtigung zum Auflisten aller Monitore in einem Konto und deren Status	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für eine Ressource	Lesen	Monitor*		
StartQuery	Gewährt die Berechtigung zum Starten einer Datenabfrage für einen Monitor	Lesen	Monitor*		
StopQuery	Gewährt die Berechtigung zum Stoppen einer Datenabfrage für einen Monitor	Lesen	Monitor*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Ressource.	Markieren	Monitor*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Ressource	Tagging	Monitor*		
				aws:TagKeys	
UpdateMonitor	Gewährt die Berechtigung zum Aktualisieren eines Monitors	Schreiben	Monitor*		

Von Amazon CloudWatch Internet Monitor definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
HealthEvent	`arn:${Partition}:internetmonitor:${Region}:${Account}:monitor/${MonitorName}/health-event/${EventId}`	

Ressourcentypen	ARN	Bedingungsschlüssel
Monitor	`arn:${Partition}:internetmonitor:${Region}:${Account}:monitor/${MonitorName}`	aws:ResourceTag/${TagKey}
InternetEvent	`arn:${Partition}:internetmonitor::${Account}:internet-event/${InternetEventId}`	

Zustandstasten für Amazon CloudWatch Internet Monitor

Amazon CloudWatch Internet Monitor definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert Aktionen nach den Tag-Schlüsseln in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CloudWatch Logs

Amazon CloudWatch Logs (Servicepräfix: `logs`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon CloudWatch Logs definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateKmsKey	Gewährt die Berechtigung zum Zuordnen des angegebenen AWS Key-Management-Service (AWS KMS)-Kundenmasterschlüssels (CMK) der angegebenen Protokollgruppe	Schreiben	log-group *		
CancelExportTask	Gewährt die Berechtigung zum Abbrechen einer Exportaufgabe, wenn diese den Status PENDING oder RUNNING hat	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDelivery	Gewährt die Berechtigung zum Erstellen einer Sendung, die eine Zustellquelle mit einem Zustellziel verbindet	Schreiben	delivery*		
			delivery-destination*		
			delivery-source*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateExportTask	Gewährt die Berechtigung zum Erstellen eines ExportTask , mit dem Sie Daten effizient aus einer Protokollgruppe in Ihren Amazon S3-Bucket exportieren können	Schreiben	log-group*		
CreateLogAnomalyDetector	Gewährt die Berechtigung zum Erstellen eines Protokollanomalie-Detektors	Schreiben	log-group*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateLogDelivery [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer Protokollieferung	Schreiben			
CreateLogGroup	Gewährt die Berechtigungen zum Erstellen einer neuen Protokollgruppe mit dem angegebenen Namen	Schreiben	log-group*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateLogStream	Gewährt die Berechtigung zum Erstellen eines neuen Protokoll-Streams mit dem angegebenen Namen	Schreiben	log-stream*		
DeleteAccountPolicy	Gewährt die Berechtigung, eine Datenschutzrichtlinie zu löschen, die einem Konto angefügt ist	Schreiben			
DeleteDataProtectionPolicy	Gewährt die Berechtigung zum Löschen einer Datenschutzrichtlinie, die einer Protokollgruppe zugeordnet ist	Schreiben	log-group*		
DeleteDelivery	Gewährt die Berechtigung zum Löschen einer Zustellung	Schreiben	delivery*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteDeliveryDestination	Gewährt die Berechtigung zum Löschen eines Zustellziels, nachdem alle zugehörigen Sendungen gelöscht wurden	Schreiben	delivery-destination*		
DeleteDeliveryDestinationPolicy	Gewährt die Berechtigung zum Löschen einer Zustellziel-Richtlinie, die einem Zustellziel zugeordnet ist	Schreiben	delivery-destination*		
DeleteDeliverySource	Gewährt die Berechtigung zum Löschen einer Zustellungsquelle, nachdem alle zugehörigen Sendungen gelöscht wurden	Schreiben	delivery-destination*		
DeleteDestination	Gewährt die Berechtigung zum Löschen des Ziels mit dem angegebenen Namen	Schreiben	destination*		
DeleteLogAnomalyDetector	Gewährt die Berechtigung zum Löschen eines Protokoll anomalie-Detektors	Schreiben	anomaly-detector*		
DeleteLogDelivery [nur Berechtigung]	Gewährt die Berechtigung zum Löschen von Protokoll bereitstellungsinformationen über die angegebene Protokoll bereitstellung	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteLogGroup	Gewährt die Berechtigung zum Löschen der Protokollgruppe mit dem angegebenen Namen	Schreiben	log-group*		
DeleteLogStream	Gewährt die Berechtigung zum Löschen eines Protokollstreams	Schreiben	log-stream*		
DeleteMetricFilter	Gewährt die Berechtigung zum Löschen eines Kennzahlenfilters mit der angegebenen Protokollgruppe	Schreiben	log-group*		
DeleteQueryDefinition	Gewährt die Berechtigung zum Löschen einer gespeicherten CloudWatch Logs-Insights-Abfragedefinition	Schreiben			
DeleteResourcePolicy	Gewährt die Berechtigung zum Löschen von Ressourcenrichtlinien von diesem Konto	Berechtigungsverwaltung			
DeleteRetentionPolicy	Gewährt die Berechtigung zum Löschen der Aufbewahrungsrichtlinie der angegebenen Protokollgruppe	Schreiben	log-group*		
DeleteSubscriptionFilter	Gewährt die Berechtigung zum Löschen eines Abonnementfilters mit der angegebenen Protokollgruppe	Schreiben	log-group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeAccountPolicies	Gewährt die Berechtigung, eine Datenschutzrichtlinie abzurufen, die einem Konto angefügt ist	Auflisten			
DescribeDeliveries	Gewährt die Berechtigung zum Abrufen einer Liste von Zustellungen eines Kontos	Auflisten			
DescribeDeliveryDestinations	Gewährt die Berechtigung zum Abrufen einer Liste der Zustellziele eines Kontos	Auflisten			
DescribeDeliverySources	Gewährt die Berechtigung zum Abrufen einer Liste der Zustellquellen in einem Konto	Auflisten			
DescribeDestinations	Gewährt die Berechtigung zum Zurückgeben von allen Ziele, die dem anfordernden AWS-Konto zugeordnet sind	Auflisten			
DescribeExportTasks	Gewährt die Berechtigung zum Zurückgeben von allen Exportaufgaben, die dem anfordernden AWS-Konto zugeordnet sind	Auflisten			
DescribeLogGroups	Gewährt die Berechtigung zum Zurückgeben von allen Protokollgruppen, die dem anfordernden AWS-Konto zugeordnet sind	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeLogStreams	Gewährt die Berechtigung zum Zurückgeben von allen Protokoll-Streams, die der angegebenen Protokollgruppe zugeordnet sind	Auflisten	log-group *		
DescribeMetricFilters	Gewährt die Berechtigung zum Zurückgeben von allen Kennzahlenfiltern, die der angegebenen Protokollgruppe zugeordnet sind	Auflisten	log-group *		
DescribeQueries	Gewährt die Berechtigung zum Zurückgeben einer Liste von CloudWatch Logs-Insights-Abfragen, die geplant sind, ausgeführt werden oder kürzlich in diesem Konto ausgeführt wurden	Auflisten			
DescribeQueryDefinitions	Gewährt die Berechtigung zum Zurückgeben einer paginierten Liste Ihrer gespeicherten CloudWatch Logs-Insights-Abfragedefinitionen	Auflisten			
DescribeResourcePolicies	Gewährt die Berechtigung zum Zurückgeben von allen Ressourcenrichtlinien in diesem Konto	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeSubscriptionFilters	Gewährt die Berechtigung zum Zurückgeben von allen Abonnementfiltern, die der angegebenen Protokollgruppe zugeordnet sind	Auflisten	log-group*		
DisassociateKmsKey	Gewährt die Berechtigung zum Aufheben der Mapping des AWS Key Management Service (AWS KMS)-Kundenmasterschlüssels (CMK) zur angegebenen Protokollgruppe	Schreiben	log-group*		
FilterLogEvents	Gewährt die Berechtigung zum Abrufen von Protokollereignissen, optional gefiltert durch ein Filtermuster aus der angegebenen Protokollgruppe	Lesen	log-group*		
GetDataProtectionPolicy	Gewährt die Berechtigung zum Abrufen einer Datenschutzrichtlinie, die einer Protokollgruppe zugeordnet ist	Lesen	log-group*		
GetDelivery	Gewährt die Berechtigung zum Abrufen einer einzelnen Zustellung	Lesen	delivery*		
GetDeliveryDestination	Gewährt die Berechtigung zum Abrufen eines einzelnen Zustellziels	Lesen	delivery-destination*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDeliveryDestinationPolicy	Gewährt die Berechtigung zum Abrufen einer Zustellziel-Richtlinie, die an ein Zustellziel angehängt ist	Lesen	delivery-destination*		
GetDeliverySource	Gewährt die Berechtigung zum Abrufen einer einzelnen Zustellquelle	Lesen	delivery-source*		
GetLogAnomalyDetector	Gewährt die Berechtigung, eine Liste von Protokoll anomalie-Detektors abzurufen	Lesen	anomaly-detector*		
GetLogDelivery [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Informationen über die angegebene Protokollbereitstellung	Lesen			
GetLogEvents	Gewährt die Berechtigung zum Abrufen von Protokoll ereignissen aus dem angegebenen Protokollstream	Lesen	log-stream*		
GetLogGroupFields	Gewährt die Berechtigung zum Zurückgeben einer Liste der Felder, die in Protokollereignissen der angegebenen Protokollgruppe enthalten sind, zusammen mit dem Prozentsatz der Protokollereignisse, die in den einzelnen Feldern eingeschlossen sind	Lesen	log-group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetLogRecord	Gewährt die Berechtigung zum Abrufen von allen Feldern und Werten eines einzelnen Protokollereignisses	Lesen	log-group *		
GetQueryResults	Gewährt die Berechtigung zum Zurückgeben von Ergebnissen aus der angegebenen Abfrage	Lesen	log-group *		
Link [nur Berechtigung]	Gewährt die Berechtigung zum Freigeben von CloudWatch Ressourcen für ein Überwachungskonto	Schreiben			
ListAnomalies	Gewährt die Berechtigung zum Auflisten aller bei der AWS-Konto Anforderung festgestellten Anomalien	Auflisten	anomaly-detector		
ListLogAnomalyDetectors	Gewährt die Berechtigung zum Zurückgeben von allen Anomaliedetektoren, die dem anfordernden AWS-Konto zugeordnet sind	Auflisten	log-group		
ListLogDeliveries [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von allen Protokollbereitstellungen für das angegebene Konto und/oder die Protokollquelle	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für die angegebene Ressource	Auflisten	anomaly-detector		
			delivery		
			delivery-destination		
			delivery-source		
			destination		
			log-group		
ListTagsLogGroup	Gewährt die Berechtigung zum Auflisten der Tags für die spezifische Protokollgruppe	Auflisten	log-group *		
PutAccountPolicy	Gewährt die Berechtigung, eine Datenschutzrichtlinie auf Kontoebene anzufügen, um vertrauliche Informationen aus Protokollereignissen zu erkennen und zu redigieren	Schreiben			
PutDataProtectionPolicy	Gewährt die Berechtigung zum Anhängen einer Datenschutzrichtlinie, um vertrauliche Informationen aus Protokollereignissen zu erkennen und zu redigieren	Schreiben	log-group *		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutDeliveryDestination	Gewährt die Berechtigung zum Erstellen/Aktualisieren eines Zustellziels	Schreiben	delivery-destination*		
				aws:TagKeys aws:RequestTag/${TagKey} logs:DeliveryDestinationResourceArn	
PutDeliveryDestinationPolicy	Gewährt die Berechtigung zum Anhängen einer Zustellziel-Richtlinie für ein Zustellziel	Schreiben	delivery-destination*		
PutDeliverySource	Gewährt die Berechtigung zum Erstellen/Aktualisieren einer Zustellquelle	Schreiben	delivery-source*		
				aws:TagKeys aws:RequestTag/${TagKey} logs:LogGeneratingResourceArns	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutDestination	Gewährt die Berechtigung zum Erstellen oder Aktualisieren eines Ziels	Schreiben	destination*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey}	
PutDestinationPolicy	Gewährt die Berechtigung zum Erstellen und Aktualisieren einer Zugriffsrichtlinie, die einem bestehenden Ziel zugeordnet ist	Schreiben	destination*		
PutLogEvents	Gewährt die Berechtigung zum Hochladen eines Batches von Protokollereignissen in den angegebenen Protokoll stream	Schreiben	log-stream*		
PutMetricFilter	Gewährt die Berechtigung zum Erstellen oder Aktualisieren eines Kennzahlenfilters und ordnet ihn der angegeben en Protokollgruppe zu	Schreiben	log-group*		
PutQueryDefinition	Gewährt die Berechtigung zum Erstellen oder Aktualisieren einer Abfragedefinition	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutResourcePolicy	Gewährt die Berechtigung zum Erstellen oder Aktualisieren einer Ressourcenrichtlinie, die es anderen AWS-Services ermöglicht, Protokollereignisse in dieses Konto zu schreiben	Berechtigungsverwaltung			
PutRetentionPolicy	Gewährt die Berechtigung zum Festlegen der Aufbewahrungsdauer der angegebenen Protokollgruppe	Schreiben	log-group *		
PutSubscriptionFilter	Gewährt die Berechtigung zum Erstellen oder Aktualisieren eines Abonnementfilter und ordnet es einer angegebenen Protokollgruppe zu	Schreiben	log-group *		iam:PassRole
			destination		
StartLiveTail	Gewährt die Berechtigung zum Starten einer Live-Tail-Sitzung in - CloudWatch Protokollen	Lesen	log-group *		
StartQuery	Gewährt die Berechtigung zum Planen einer Abfrage einer Protokollgruppe mithilfe von CloudWatch Logs Insights	Lesen	log-group *		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopLiveTail [nur Berechtigung]	Gewährt die Berechtigung zum Beenden einer Live-Tail-Sitzung in CloudWatch-Logs, die gerade ausgeführt wird	Lesen			
StopQuery	Gewährt die Berechtigung zum Stoppen einer laufenden CloudWatch Logs-Insights-Abfrage	Lesen			
TagLogGroup	Gewährt die Berechtigung zum Hinzufügen oder Aktualisieren der angegebenen Tags für die angegebene Protokollgruppe	Tagging	log-group *		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource	Gewährt die Berechtigung zum Hinzufügen oder Aktualisieren der angegebenen Tags zur angegebenen Ressource	Tagging	anomaly-detector		
			delivery		
			delivery-destination		
			delivery-source		
			destination		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			log-group		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestMetricFilter	Gewährt die Berechtigung zum Testen des Filtermuster eines Kennzahlenfilters anhand einer Stichprobe von Protokollereignismeldungen	Lesen			
Unmask [nur Berechtigung]	Gewährt die Berechtigung unmaskierte Protokollereignisse abzurufen, die mit einer Datenschutzrichtlinie redigiert wurden	Lesen	log-group *		
UntagLogGroup	Gewährt die Berechtigung zum Entfernen der angegebenen Tags aus der angegebenen Protkollgruppe	Tagging	log-group *		
				aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen der angegebenen Tags aus der angegebenen Ressource	Tagging	anomaly-detector		
			delivery		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			delivery-destination		
			delivery-source		
			destination		
			log-group		
				aws:TagKeys	
UpdateAnomaly	Gewährt die Berechtigung zum Aktualisieren einer Anomalie, die von einem Protokollanomalie-Detektor berichtet wurde	Schreiben	anomaly-detector*		
UpdateLogAnomalyDetector	Gewährt die Berechtigung, einen Protokollanomalie-Detektor zu aktualisieren	Schreiben	anomaly-detector*		
UpdateLogDelivery [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren der Informationen über die angegebene Protokollbereitstellung	Schreiben			

Von Amazon CloudWatch Logs definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
log-group	`arn:${Partition}:logs:${Region}:${Account}:log-group:${LogGroupName}`	aws:ResourceTag/${TagKey}
log-stream	`arn:${Partition}:logs:${Region}:${Account}:log-group:${LogGroupName}:log-stream:${LogStreamName}`	aws:ResourceTag/${TagKey}
destination	`arn:${Partition}:logs:${Region}:${Account}:destination:${DestinationName}`	aws:ResourceTag/${TagKey}
delivery-source	`arn:${Partition}:logs:${Region}:${Account}:delivery-source:${DeliverySourceName}`	aws:ResourceTag/${TagKey}
delivery	`arn:${Partition}:logs:${Region}:${Account}:delivery:${DeliveryName}`	aws:ResourceTag/${TagKey}
delivery-destination	`arn:${Partition}:logs:${Region}:${Account}:delivery-destination:${DeliveryDestinationName}`	aws:ResourceTag/${TagKey}
anomaly-detector	`arn:${Partition}:logs:${Region}:${Account}:anomaly-detector:${DetectorId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon CloudWatch Logs

Amazon CloudWatch Logs definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString
logs:DeliveryDestinationResourceArn	Filtert den Zugriff durch den Logziel-ARN, der in der Anforderung übergeben wird	ARN
logs:LogGenerating ResourceArns	Filtert den Zugriff durch die ARNs der Protokollgenerierungsressource, die in der Anforderung übergeben werden	ArrayOfARN

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CloudWatch Network Monitor

Amazon CloudWatch Network Monitor (Servicepräfix: `networkmonitor`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon CloudWatch Network Monitor definierte Aktionen
- Von Amazon CloudWatch Network Monitor definierte Ressourcentypen
- Bedingungsschlüssel für Amazon CloudWatch Network Monitor

Von Amazon CloudWatch Network Monitor definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateMonitor	Gewährt die Berechtigung zum Erstellen eines Monitors	Schreiben	monitor*		
CreateProbe	Gewährt die Berechtigung zum Erstellen einer Probe	Schreiben			
DeleteMonitor	Gewährt die Berechtigung zum Löschen eines Monitors	Schreiben	monitor*		
DeleteProbe	Gewährt die Berechtigung zum Löschen einer Probe	Schreiben	probe*		
GetMonitor	Gewährt die Berechtigung zum Abrufen von Informationen über einen Monitor	Lesen	monitor*		
GetProbe	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Probe	Lesen	probe*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListMonitors	Gewährt die Berechtigung zum Auflisten aller Monitore in einem Konto und deren Status	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für eine Ressource	Lesen	monitor		
			probe		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Ressource.	Markieren	monitor		
			probe		
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Ressource	Tagging	monitor		
			probe		
				aws:TagKeys	
UpdateMonitor	Gewährt die Berechtigung zum Aktualisieren eines Monitors	Schreiben	monitor*		
UpdateProbe	Gewährt die Berechtigung zum Aktualisieren einer Probe	Schreiben	probe*		

Von Amazon CloudWatch Network Monitor definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
monitor	`arn:${Partition}:networkmonitor:${Region}:${Account}:monitor/${MonitorName}`	aws:ResourceTag/${TagKey}
probe	`arn:${Partition}:networkmonitor:${Region}:${Account}:probe/${ProbeId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon CloudWatch Network Monitor

Amazon CloudWatch Network Monitor definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tag-Schlüssel-Wert-Paare in der Anforderung	String
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüsselwertpaaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert Aktionen nach den Tag-Schlüsseln in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CloudWatch Observability Access Manager

Amazon CloudWatch Observability Access Manager (Servicepräfix: `oam`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon CloudWatch Observability Access Manager definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie

den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateLink	Gewährt die Berechtigung zum Erstellen einer Verknüpfung zwischen einem Überwachungs-Konto und einem Quellkonto für die kontoübergreifende Überwachung	Schreiben	Sink*		oam:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys oam:ResourceTypes	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSink	Gewährt die Berechtigung zum Erstellen einer Senke in einem Konto, sodass sie als Überwachungs-Konto für die kontenübergreifende Überwachung verwendet werden kann	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	oam:TagResource
DeleteLink	Gewährt die Berechtigung zum Löschen einer Verknüpfung zwischen einem Überwachungs-Konto und einem Quellkonto für die kontoübergreifende Überwachung	Schreiben	Link*		
				aws:ResourceTag/${TagKey}	
DeleteSink	Gewährt die Berechtigung zum Löschen einer kontoübergreifenden Überwachungssenke in einem Überwachungs-Konto	Schreiben	Sink*		
				aws:ResourceTag/${TagKey}	
GetLink	Gewährt die Berechtigung zum Abrufen von vollständigen Informationen über einen kontoübergreifenden Überwachungslink	Lesen	Link*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetSink	Gewährt die Berechtigung zum Abrufen von vollständigen Informationen über eine kontoübergreifende Überwachungssenke	Lesen	Sink*		
				aws:ResourceTag/${TagKey}	
GetSinkPolicy	Gewährt die Berechtigung zum Abrufen von Informationen für die IAM-Richtlinie für eine kontoübergreifende Überwachungssenke	Lesen	Sink*		
				aws:ResourceTag/${TagKey}	
ListAttachedLinks	Gewährt die Berechtigung zum Abrufen einer Liste von Links, die für eine kontoübergreifende Überwachungssenke verknüpft sind	Lesen	Sink*		
				aws:ResourceTag/${TagKey}	
ListLinks	Gewährt die Berechtigung zum Abrufen der ARNs der kontoübergreifenden Überwachungslinks in diesem Konto	Lesen			
ListSinks	Gewährt die Berechtigung zum Abrufen von der ARNs der kontenübergreifenden Überwachungssenken in diesem Konto	Lesen			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für eine Ressource	Lesen	Link		
			Sink		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutSinkPolicy	Gewährt die Berechtigung zum Erstellen oder Aktualisieren der IAM-Richtlinie für eine kontoübergreifende Überwachungssenke	Schreiben	Sink*		
				aws:ResourceTag/${TagKey}	
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren	Link		
			Sink		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Markierung	Link		
			Sink		
				aws:TagKeys	
UpdateLink	Gewährt die Berechtigung zum Aktualisieren einer vorhandenen Verknüpfung zwischen einem Überwachungs-Konto und einem Quellkonto	Schreiben	Link*		
				aws:ResourceTag/${TagKey} oam:ResourceTypes	

Von Amazon CloudWatch Observability Access Manager definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Link	`arn:${Partition}:oam:${Region}:${Account}:link/${ResourceId}`	aws:ResourceTag/${TagKey}
Sink	`arn:${Partition}:oam:${Region}:${Account}:sink/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon CloudWatch Observability Access Manager

Amazon CloudWatch Observability Access Manager definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString
oam:ResourceTypes	Filtert den Zugriff nach dem Vorhandensein von Ressourcentypen in der Anfrage	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS CloudWatch RUM

AWS CloudWatchRUM (Servicepräfix: `rum`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS CloudWatch RUM definierte Aktionen
- Von AWS CloudWatch RUM definierte Ressourcentypen
- Bedingungsschlüssel für AWS CloudWatch RUM

Von AWS CloudWatch RUM definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchCreateRumMetricDefinitions	Gewährt die Berechtigung zum Erstellen von Rum-Metrik-Definitionen	Schreiben	AppMonitorResource*		
BatchDeleteRumMetricDefinitions	Gewährt die Berechtigung zum Entfernen von Rum-Metrik-Definitionen	Schreiben	AppMonitorResource*		
BatchGetRumMetricDefinitions	Gewährt die Berechtigung zum Abrufen von Rum-Metrik-Definitionen	Lesen	AppMonitorResource*		
CreateAppMonitor	Gewährt die Berechtigung zum Erstellen von appMonitor-Metadaten	Schreiben	AppMonitorResource*		iam:CreateServiceLinkedRole iam:GetRole
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAppMonitor	Gewährt die Berechtigung zum Löschen von appMonitor-Metadaten	Schreiben	AppMonitorResource*		
DeleteRumMetricsDestination	Gewährt die Berechtigung zum Löschen von Zielen für Rum-Metriken	Schreiben	AppMonitorResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAppMonitor	Gewährt die Berechtigung zum Abrufen von appMonitor-Metadaten	Lesen	AppMonitorResource*		
GetAppMonitorData	Gewährt die Berechtigung zum Abrufen von appMonitor-Daten	Lesen	AppMonitorResource*		
ListAppMonitors	Gewährt die Berechtigung zum Auflisten von appMonitor-Metadaten	Auflisten			
ListRumMetricsDestinations	Gewährt die Berechtigung zum Auflisten von Zielen für Rum-Metriken	Lesen	AppMonitorResource*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für Ressourcen	Lesen			
PutRumEvents	Gewährt die Berechtigung zum Ablegen von RUM-Ereignissen für appMonitor	Schreiben	AppMonitorResource*		
PutRumMetricsDestination	Gewährt die Berechtigung zum Setzen von Zielen für Rum-Metriken	Schreiben	AppMonitorResource*		
TagResource	Gewährt die Berechtigung zum Markieren von Ressourcen	Markierung	AppMonitorResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung von Ressourcen	Markierung	AppMonitorResource*		
				aws:TagKeys	
UpdateAppMonitor	Gewährt die Berechtigung zum Aktualisieren von appMonitor-Metadaten	Schreiben	AppMonitorResource*		iam:CreateServiceLinkedRole iam:GetRole
UpdateRumMetricDefinition	Gewährt die Berechtigung zum Aktualisieren der Rum-Metrik-Definition	Schreiben	AppMonitorResource*		

Von AWS CloudWatch RUM definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
AppMonitorResource	`arn:${Partition}:rum:${Region}:${Account}:appmonitor/${Name}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS CloudWatch RUM

AWS CloudWatch RUM definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach den Tags, die von der Anforderung im Auftrag des IAM-Prinzipals weitergeleitet werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach den Tags, die der Ressource zugeordnet sind, die die Anforderung im Auftrag des IAM-Prinzipals tätigen	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach den Tag-Schlüsseln, die von der Anforderung im Auftrag des IAM-Prinzipals weitergeleitet werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CloudWatch Synthetics

Amazon CloudWatch Synthetics (Servicepräfix: `synthetics`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon CloudWatch Synthetics definierte Aktionen
- Ressourcentypen, die von Amazon CloudWatch Synthetics definiert werden
- Bedingungsschlüssel für Amazon CloudWatch Synthetics

Von Amazon CloudWatch Synthetics definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateResource	Gewährt die Berechtigung, einer Ressource eine Gruppe zuzuordnen	Schreiben	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
CreateCanary	Gewährt die Berechtigung zum Erstellen eines Canary	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGroup	Gewährt die Berechtigung zum Erstellen einer Gruppe	Schreiben		aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
DeleteCanary	Gewährt die Berechtigung zum Löschen eines Canary. Amazon Synthetics löscht alle Ressourcen mit Ausnahme der Lambda-Funktion und der CloudWatch-Alarme, falls Sie diese erstellt haben.	Schreiben	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteGroup	Gewährt die Berechtigung zum Löschen einer Gruppe	Schreiben	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
DescribeCanaries	Gewährt die Berechtigung zum Auflisten von Informationen aller Canarys	Lesen		synthetics:Names	
DescribeCanariesLastRun	Gewährt die Berechtigung zum Auflisten von Informationen über den letzten Testlauf, der allen Canarys zugeordnet ist	Lesen		synthetics:Names	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeRuntimeVersions	Gewährt die Berechtigung zum Auflisten von Informationen über Synthetics Canary-Laufzeitversionen	Lesen			
DisassociateResource	Gewährt die Berechtigung, eine Gruppe von einer Ressource zu trennen	Schreiben	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
GetCanary	Gewährt die Berechtigung zum Anzeigen der Details eines Canary	Lesen	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
GetCanaryRuns	Gewährt die Berechtigung zum Auflisten von Informationen über alle Testläufe, die einem Canary zugeordnet sind	Lesen	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
GetGroup	Gewährt die Berechtigung zum Anzeigen der Gruppendetails	Lesen	group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} aws:TagKeys	
ListAssociatedGroups	Gewährt die Berechtigung zum Auflisten von Informationen über die Gruppen, die einem Canary zugeordnet sind	Auflisten	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ListGroupResources	Gewährt die Berechtigung zum Auflisten von Informationen über Canaries in einer Gruppe	Auflisten	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ListGroups	Gewährt die Berechtigung zum Auflisten von Informationen aller Gruppen	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten aller Tags und Werte, die einer Ressource zugeordnet sind	Lesen	canary		
			group		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartCanary	Gewährt die Berechtigung, einen Canary zu starten, damit Amazon CloudWatch Synthetics mit der Überwachung einer Website beginnt	Write	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
StopCanary	Gewährt die Berechtigung zum Beenden eines Canarys	Schreiben	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
TagResource	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Tags zu einer Ressource	Markieren	canary		
			group		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung, ein oder mehrere Tags aus einer Ressource zu entfernen	Markierung	canary		
			group		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCanary	Gewährt die Berechtigung zum Aktualisieren eines Canarys	Write	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Ressourcentypen, die von Amazon CloudWatch Synthetics definiert werden

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
canary	`arn:${Partition}:synthetics:${Region}:${Account}:canary:${CanaryName}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
group	`arn:${Partition}:synthetics:${Region}:${Account}:group:${GroupId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon CloudWatch Synthetics

Amazon CloudWatch Synthetics definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüsseln, die in der Anforderung übergeben werden.	ArrayOfString
synthetics:Names	Filtert den Zugriff basierend auf dem Namen der canary	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS CodeArtifact

AWS CodeArtifact (Servicepräfix: `codeartifact`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS CodeArtifact definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateExternalConnection	Gewährt die Berechtigung zum Hinzufügen einer externen Verbindung zu einem Repository.	Write	repository*		
AssociateWithDownstreamRepository	Gewährt die Berechtigung, ein vorhandenes Repository als Upstream-Repository einem anderen Repository zuzuordnen.	Schreiben	repository*		
CopyPackageVersions	Gewährt die Berechtigung zum Kopieren von Paketversionen aus einem Repository	Schreiben	package*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	in ein anderes Repository in derselben Domain		repository*		
CreateDomain	Gewährt die Berechtigung zum Erstellen einer neuen Domain	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePackageGroup	Gewährt die Berechtigung zum Erstellen einer Paketgruppe	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRepository	Gewährt die Berechtigung zum Erstellen eines neuen Repositorys.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDomain	Gewährt die Berechtigung zum Löschen einer Domain	Write	domain*		
DeleteDomainPermissionsPolicy	Gewährt die Berechtigung zum Löschen des Ressourcenrichtliniensatzes für eine Domain	Berechtigungsverwaltung	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeletePackage	Gewährt die Berechtigung zum Löschen eines Pakets	Schreiben	package*		
DeletePackageGroup	Gewährt die Berechtigung zum Löschen einer Paketgruppe	Schreiben	package-group*		
DeletePackageVersions	Gewährt die Berechtigung zum Löschen von Paketversionen.	Write	package*		
DeleteRepository	Gewährt die Berechtigung zum Löschen eines Repositorys.	Write	repository*		
DeleteRepositoryPermissionsPolicy	Gewährt die Berechtigung zum Löschen des Ressourcenrichtliniensatzes in einem Repository.	Berechtigungsverwaltung	repository*		
DescribeDomain	Gewährt die Berechtigung zum Zurückgeben von Informationen zu einer Domain	Lesen	domain*		
DescribePackage	Erteilung der Berechtigung zum Abruf von Informationen über ein Paket	Lesen	package*		
DescribePackageGroup	Gewährt die Berechtigung zum Zurückgeben detaillierter Informationen zu einer Paketgruppe	Lesen	package-group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribePackageVersion	Gewährt die Berechtigung zum Zurückgeben von Informationen über eine Paketversion.	Read	package*		
DescribeRepository	Gewährt die Berechtigung, detaillierte Informationen über ein Repository zurückzugeben.	Read	repository*		
DisassociateExternalConnection	Gewährt die Berechtigung zum Aufheben der Mapping einer externen Verbindung zu einem Repository.	Write	repository*		
DisposePackageVersions	Gewährt die Berechtigung, den Status von Paketversionen auf „Disposed“ festzulegen und ihre Assets zu löschen.	Schreiben	package*		
GetAssociatedPackageGroup	Gewährt die Berechtigung zum Zurückgeben der zugeordneten Paketgruppe eines Pakets	Lesen	package-group*		
GetAuthorizationToken	Gewährt die Berechtigung zum Generieren eines temporären Authentifizierungstokens für den Zugriff auf Repositoys in einer Domain	Read	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDomainPermissionsPolicy	Gewährt die Berechtigung zum Zurückgeben der Ressourcenrichtlinie einer Domain.	Read	domain*		
GetPackageVersionAsset	Gewährt die Berechtigung zum Zurückgeben eines Assets (oder einer Datei), das Teil einer Paketversion ist.	Read	package*		
GetPackageVersionReadme	Gewährt die Berechtigung zum Zurückgeben der Readme-Datei einer Paketversion.	Read	package*		
GetRepositoryEndpoint	Gewährt die Berechtigung zum Zurückgeben eines Endpunkts für ein Repository.	Read	repository*		
GetRepositoryPermissionsPolicy	Gewährt die Berechtigung zum Zurückgeben der Ressourcenrichtlinie eines Repositorys.	Lesen	repository*		
ListAllowedRepositoriesForGroup	Gewährt die Berechtigung zum Auflisten der zulässigen Repositorys für eine Paketgruppe	Auflisten	package-group*		
ListAssociatedPackages	Gewährt die Berechtigung zum Auflisten der Pakete, die einer Paketgruppe zugeordnet sind	Auflisten	package-group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDomains	Gewährt die Berechtigung zum Auflisten der Domains im des aktuellen Benutzers AWS-Konto	Auflisten			
ListPackageGroups	Gewährt die Berechtigung zum Auflisten der Paketgruppen in einer Domain	Auflisten	domain*		
ListPackageVersionAssets	Gewährt die Berechtigung zum Auflisten der Assets einer Paketversion.	List	package*		
ListPackageVersionDependencies	Gewährt die Berechtigung, die direkten Abhängigkeiten einer Paketversion aufzulisten.	List	package*		
ListPackageVersions	Gewährt die Berechtigung zum Auflisten der Versionen eines Pakets.	List	package*		
ListPackages	Gewährt die Berechtigung zum Auflisten der Pakete in einem Repository.	List	repository*		
ListRepositories	Gewährt die Berechtigung, die vom aufrufenden Konto verwalteten Repositorys aufzulisten	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListRepositoriesInDomain	Gewährt die Berechtigung zum Auflisten der Repositorys in einer Domain	Auflisten	domain*		
ListSubPackageGroups	Gewährt die Berechtigung zum Auflisten der Unterpaketgruppen für eine übergeordnete Paketgruppe	Auflisten	package-group*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine CodeArtifact Ressource	Auflisten	domain		
			package-group		
			repository		
PublishPackageVersion	Gewährt die Berechtigung zum Veröffentlichen von Assets und Metadaten auf einem Repository-Endpunkt.	Write	package*		
PutDomainPermissionsPolicy	Gewährt die Berechtigung zum Anfügen einer Ressourcenrichtlinie an eine Domain	Write	domain*		
PutPackageMetadata	Gewährt die Berechtigung zum Hinzufügen, Ändern oder Entfernen von Paketmetadaten mithilfe eines Repository-Endpunkts.	Schreiben	package*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutPackageOriginConfiguration	Erteilung der Berechtigung zum Festlegen der Ursprungskonfiguration für ein Paket	Schreiben	package*		
PutRepositoryPermissionsPolicy	Gewährt die Berechtigung zum Anfügen einer Ressourcenrichtlinie an ein Repository.	Write	repository*		
ReadFromRepository	Gewährt die Berechtigung zum Zurückgeben von Paket-Assets und -Metadaten von einem Repository-Endpunkt.	Lesen	repository*		
TagResource	Gewährt die Berechtigung zum Markieren einer CodeArtifact Ressource	Tagging	domain		
			package-group		
			repository		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen eines Tags aus einer CodeArtifact Ressource	Tagging	domain		
			package-group		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			repository		
				aws:TagKeys	
UpdatePackageGroup	Gewährt die Berechtigung zum Ändern der Eigenschaften einer Paketgruppe	Schreiben	package-group*		
UpdatePackageGroupOriginConfiguration	Gewährt die Berechtigung zum Ändern der Paketursprungskonfiguration einer Paketgruppe	Schreiben	package-group*		
UpdatePackageVersionsStatus	Gewährt die Berechtigung zum Ändern des Status einer oder mehrerer Versionen eines Pakets.	Write	package*		
UpdateRepository	Gewährt die Berechtigung zum Ändern der Eigenschaften eines Repositorys.	Schreiben	repository*		

Von AWS CodeArtifact definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

> **Note**
>
> Der ARN der Paketgruppen-Ressource muss ein codiertes Paketgruppenmuster verwenden.

Ressource ntypen	ARN	Bedingungsschlüssel
domain	`arn:${Partition}:codeartifact:${Region}:${Account}:domain/${DomainName}`	aws:ResourceTag/${TagKey}
repository	`arn:${Partition}:codeartifact:${Region}:${Account}:repository/${DomainName}/${RepositoryName}`	aws:ResourceTag/${TagKey}
package-group	`arn:${Partition}:codeartifact:${Region}:${Account}:package-group/${DomainName}${EncodedPackageGroupPattern}`	aws:ResourceTag/${TagKey}
package	`arn:${Partition}:codeartifact:${Region}:${Account}:package/${DomainName}/${RepositoryName}/${PackageFormat}/${PackageNamespace}/${PackageName}`	

Bedingungsschlüssel für AWS CodeArtifact

AWS CodeArtifact definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	String
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS CodeBuild

AWS CodeBuild (Servicepräfix: `codebuild`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS CodeBuild definierte Aktionen
- Von AWS CodeBuild definierte Ressourcentypen
- Bedingungsschlüssel für AWS CodeBuild

Von AWS CodeBuild definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den

Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchDeleteBuilds	Gewährt die Berechtigung zum Löschen eines oder mehrerer Builds.	Schreiben	project*		
BatchGetBuildBatches	Gewährt die Berechtigung zum Abrufen von Informationen zu einzelnen oder mehreren Build-Batches	Lesen	project*		
BatchGetBuilds	Gewährt die Berechtigung zum Abrufen von Informationen zu einzelnen oder mehreren Builds	Lesen	project*		
BatchGetFleets	Gewährt die Berechtigung zum Zurückgeben eines Arrays der durch den Eingabeparameter angegebenen Flottenobjekte	Lesen	fleet*		
BatchGetProjects	Gewährt die Berechtigung zum Abrufen von Informationen zu einzelnen oder mehreren Build-Projekten	Lesen	project*		
BatchGetReportGroups	Gewährt die Berechtigung zum Zurückgeben eines Arrays von ReportGroup Objekten, die durch den reportGroupArns Eingabeparameter angegeben werden	Lesen	report-group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetReports	Gewährt die Berechtigung zum Zurückgeben eines Arrays der Report-Objekte, die durch den reportArns-Eingabeparameter angegeben werden	Lesen	report-group*		
BatchPutCodeCoverages [nur Berechtigung]	Gewährt die Berechtigung zum Hinzufügen oder Aktualisieren von Informationen zu einem Bericht	Schreiben	report-group*		
BatchPutTestCases [nur Berechtigung]	Gewährt die Berechtigung zum Hinzufügen oder Aktualisieren von Informationen zu einem Bericht	Schreiben	report-group*		
CreateFleet	Gewährt die Berechtigung zum Erstellen einer Datenverarbeitungsflotte	Schreiben	fleet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProject	Gewährt die Berechtigung zum Erstellen eines Build-Projekts	Schreiben	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateReport [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines Berichts. Ein Bericht wird erstellt, wenn während der Entwicklung eines Projekts die in der buildspec-Datei für eine Berichtsgruppe angegebenen Tests ausgeführt werden	Schreiben	report-group*		
CreateReportGroup	Gewährt die Berechtigung zum Erstellen einer Replikationsgruppe	Schreiben	report-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebhook	Gewährt die Berechtigung zum Erstellen eines Webhooks. Für ein vorhandenes AWS CodeBuild Build-Projekt, dessen Quellcode in einem - GitHub oder Bitbucket -Repository gespeichert ist, ermöglicht AWS CodeBuild , jedes Mal mit der Neuerstellung des Quellcodes zu beginnen, wenn eine Codeänderung in das Repository übertragen wird	Schreiben	project*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteBuildBatch	Gewährt die Berechtigung zum Löschen eines Build-Batches	Schreiben	project*		
DeleteFleet	Gewährt die Berechtigung zum Löschen einer Datenverarbeitungsflotte	Schreiben	fleet*		
DeleteOAuthToken [nur Berechtigung]	Gewährt die Berechtigung zum Löschen eines OAuth-Tokens von einem verbundenen OAuth-Drittanbieter. Wird nur in der AWS CodeBuild Konsole verwendet	Schreiben			
DeleteProject	Gewährt die Berechtigung zum Löschen eines Build-Projekts	Schreiben	project*		
DeleteReport	Gewährt die Berechtigung zum Löschen eines Berichts	Schreiben	report-group*		
DeleteReportGroup	Gewährt die Berechtigung zum Löschen einer Berichtsgruppe	Schreiben	report-group*		
DeleteResourcePolicy	Gewährt die Berechtigung zum Löschen einer Ressourcenrichtlinie für das zugeordnete Projekt oder die Berichtsgruppe	Berechtigungsverwaltung	project report-group		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteSourceCredentials	Gewährt die Berechtigung zum Löschen einer Reihe von GitHub-, GitHub Enterprise- oder Bitbucket-Quellanmeldeinformationen	Schreiben			
DeleteWebhook	Gewährt die Berechtigung zum Löschen eines Webhooks. Bei einem vorhandenen AWS CodeBuild Build-Projekt, bei dem der Quellcode in einem - GitHub oder Bitbucket -Repository gespeichert ist, AWS CodeBuild stoppt die Neuerstellung des Quellcodes jedes Mal, wenn eine Codeänderung in das Repository übertragen wird.	Schreiben	project*		
DescribeCodeCoverages	Gewährt die Berechtigung zum Zurückgeben eines Arrays von CodeCoverage Objekten	Lesen	report-group*		
DescribeTestCases	Gewährt die Berechtigung zum Zurückgeben eines Arrays von TestCase Objekten	Lesen	report-group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetReportGroupTrend	Gewährt die Berechtigung zum Analysieren und Akkumulieren von Testberichtswerten für die Testberichte in der angegebenen Berichtsgruppe	Lesen	report-group*		
GetResourcePolicy	Gewährt die Berechtigung zum Zurückgeben einer Ressourcenrichtlinie für das angegebene Projekt oder die angegebene Berichtsgruppe	Lesen	project		
			report-group		
ImportSourceCredentials	Gewährt die Berechtigung zum Importieren der Anmeldeinformationen des Quell-Repositorys für ein AWS CodeBuild-Projekt, dessen Quellcode in einem GitHub-, GitHub Enterprise- oder Bitbucket-Repository gespeichert ist	Schreiben			
InvalidateProjectCache	Gewährt die Berechtigung zum Zurücksetzen des Cache für ein Projekt	Schreiben	project*		
ListBuildBatches	Gewährt die Berechtigung zum Abrufen einer Liste von Build-Batch-IDs, wobei jede Build-Batch-ID einen einzelnen Build-Batch darstellt	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListBuildBatchesForProject	Gewährt die Berechtigung zum Abrufen einer Liste mit Build-Batch-IDs für das angegebene Build-Projekt, in der jede Build-Batch-ID einen einzelnen Build-Batch darstellt	Auflisten	project*		
ListBuilds	Gewährt die Berechtigung zum Abrufen einer Liste von Build-IDs ab, wobei jede Build-ID einen einzelnen Build darstellt	Auflisten			
ListBuildsForProject	Gewährt die Berechtigung zum Abrufen einer Liste mit Build-IDs für das angegebene Build-Projekt, in der jede Build-ID einen einzelnen Build darstellt	Auflisten	project*		
ListConnectedOAuthAccounts [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten verbundener OAuth-Drittanbieter. Wird nur in der AWS CodeBuild Konsole verwendet	Auflisten			
ListCuratedEnvironmentImages	Gewährt die Berechtigung zum Abrufen von Informationen zu Docker-Images, die von verwaltet werden AWS CodeBuild	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListFleets	Gewährt die Berechtigung zum Abrufen einer Liste der ARNs der Datenverarbeitungsflotte, wobei jeder ARN der Datenverarbeitungsflotte eine einzelne Flotte darstellt	Auflisten			
ListProjects	Gewährt die Berechtigung zum Abrufen einer Liste mit Build-Projektnamen, in der jeder Build-Projektname ein Build-Projekt darstellt	Auflisten			
ListReportGroups	Gewährt die Berechtigung zum Zurückgeben einer Liste von Berichtsgruppen-ARNs. Jeder Berichtsgruppen-ARN stellt eine Berichtsgruppe dar	Auflisten			
ListReports	Gewährt die Berechtigung zum Zurückgeben einer Liste von Berichts-ARNs. Jeder Berichts-ARN stellt einen Bericht dar	Auflisten			
ListReportsForReportGroup	Gewährt die Berechtigung zum Zurückgeben einer Liste von Berichts-ARNs, die zu der angegebenen Berichtsgruppe gehören. Jeder Berichts-ARN stellt einen Bericht dar	Auflisten	report-group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListRepositories [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der Quellcode-Repositorys eines verbundenen OAuth-Drittanbieters. Wird nur in der AWS CodeBuild Konsole verwendet	Auflisten			
ListSharedProjects	Gewährt die Berechtigung zum Zurückgeben einer Liste von Projekt-ARNs, die mit dem Anforderer geteilt wurden. Jeder Projekt-ARN stellt ein Projekt dar	Auflisten			
ListSharedReportGroups	Gewährt die Berechtigung zum Zurückgeben einer Liste von Berichtsgruppen-ARNs, die mit dem Anforderer geteilt wurden. Jeder Berichtsgruppen-ARN stellt eine Berichtsgruppe dar	Auflisten			
ListSourceCredentials	Gewährt die Berechtigung zum Zurückgeben einer Liste von SourceCredentialsInfo Objekten	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PersistOAuthToken [nur Berechtigung]	Gewährt die Berechtigung zum Speichern eines OAuth-Tokens von einem verbundenen OAuth-Drittanbieter. Wird nur in der AWS CodeBuild Konsole verwendet	Schreiben			
PutResourcePolicy	Gewährt die Berechtigung zum Erstellen einer Ressourcenrichtlinie für das zugeordnete Projekt oder die Berichtsgruppe	Berechtigungsverwaltung	project report-group		
RetryBuild	Gewährt die Berechtigung zum Neustarten eines Builds	Schreiben	project*		
RetryBuildBatch	Gewährt die Berechtigung zum Neustarten eines Build-Batches	Schreiben	project*		
StartBuild	Gewährt die Berechtigung zum Starten eines Builds.	Schreiben	project*		
StartBuildBatch	Gewährt die Berechtigung zum Starten eines Build-Batches.	Schreiben	project*		
StopBuild	Gewährt die Berechtigung für den Versuch, einen laufenden Build zu beenden.	Schreiben	project*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopBuildBatch	Gewährt die Berechtigung für den Versuch, einen laufenden Build-Batch zu beenden.	Schreiben	project*		
UpdateFleet	Gewährt die Berechtigung zum Ändern der Einstellungen einer vorhandenen Datenverarbeitungsflotte	Schreiben	fleet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateProject	Gewährt die Berechtigung zum Ändern der Einstellungen eines bestehenden Build-Projekts	Schreiben	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateProjectVisibility	Gewährt die Berechtigung zum Ändern der öffentlichen Sichtbarkeit eines Projekts und seiner Builds	Schreiben	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateReport [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren von Informationen zu einem Bericht	Schreiben	report-group*		
UpdateReportGroup	Gewährt die Berechtigung zum Ändern der Einstellungen einer vorhandenen Berichtsgruppe	Schreiben	report-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateWebhook	Gewährt die Berechtigung zum Aktualisieren des Webhooks, der einem -AWS CodeBuild Build-Projekt zugeordnet ist	Schreiben	project*		

Von AWS CodeBuild definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
build	`arn:${Partition}:codebuild:${Region}:${Account}:build/${BuildId}`	
build-batch	`arn:${Partition}:codebuild:${Region}:${Account}:build-batch/${BuildBatchId}`	
project	`arn:${Partition}:codebuild:${Region}:${Account}:project/${ProjectName}`	aws:ResourceTag/${TagKey}
report-group	`arn:${Partition}:codebuild:${Region}:${Account}:report-group/${ReportGroupName}`	aws:ResourceTag/${TagKey}
report	`arn:${Partition}:codebuild:${Region}:${Account}:report/${ReportGroupName}:${ReportId}`	
fleet	`arn:${Partition}:codebuild:${Region}:${Account}:fleet/${FleetName}:${FleetId}`	

Bedingungsschlüssel für AWS CodeBuild

AWS CodeBuild definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff danach, ob Tag-Schlüssel-Wert-Paare in der Anforderung vorhanden sind	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tag-Schlüssel-Wert-Paaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert Zugriff basierend auf dem Vorhandensein von Tag-Schlüsseln in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CodeCatalyst

Amazon CodeCatalyst (Service-Präfix:`codecatalyst`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon definierte Aktionen CodeCatalyst
- Von Amazon definierte Ressourcentypen CodeCatalyst
- Zustandsschlüssel für Amazon CodeCatalyst

Von Amazon definierte Aktionen CodeCatalyst

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen.

Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptConnection [nur Berechtigung]	Erteilt die Erlaubnis, eine Anfrage zur Verbindung dieses Kontos mit einem CodeCatalyst Amazon-Bereich anzunehmen	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
AssociateIamRoleToConnection [nur Berechtigung]	Gewährt die Berechtigung zum Zuordnen einer IAM-Rolle zu einer Verbindung	Schreiben	connections*		iam:PassRole
				aws:ResourceTag/${TagKey}	
AssociateIdentityCenterApplicationToSpace [nur Berechtigung]	Erteilt die Erlaubnis, eine IAM Identity Center-Anwendung einem CodeCatalyst Amazon-Bereich zuzuordnen	Schreiben	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
AssociateIdentityToIdentityCenterApplication [nur Berechtigung]	Erteilt die Erlaubnis, eine Identität mit einer IAM Identity Center-Anwendung für einen CodeCatalyst Amazon-Bereich zu verknüpfen	Schreiben	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
BatchAssociateIden	Erteilt die Erlaubnis, einer IAM Identity Center-Anwendung	Schreiben	identity-center-ap		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
titiesToIdentityCenterApplication [nur Berechtigung]	für einen Amazon-Bereich mehrere Identitäten zuzuordnen CodeCatalyst		plications*		
				aws:ResourceTag/${TagKey}	
BatchDisassociateIdentitiesFromIdentityCenterApplication [nur Berechtigung]	Erteilt die Erlaubnis, mehrere Identitäten von einer IAM Identity Center-Anwendung für einen Amazon-Bereich zu trennen CodeCatalyst	Schreiben	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
CreateIdentityCenterApplication [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer Anwendung für das IAM Identity Center	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSpace [nur Berechtigung]	Erteilt die Erlaubnis, einen CodeCatalyst Amazon-Bereich zu erstellen	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSpaceAdminRoleAssignment [nur Berechtigung]	Erteilt die Berechtigung, eine Administratorrollenzuweisung für einen bestimmten CodeCatalyst Amazon-Bereich und eine bestimmte IAM Identity Center-Anwendung zu erstellen	Schreiben	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
DeleteConnection [nur Berechtigung]	Gewährt die Berechtigung zum Löschen einer Verbindung.	Schreiben	connections*		
				aws:ResourceTag/${TagKey}	
DeleteIdentityCenterApplication [nur Berechtigung]	Gewährt die Berechtigung zum Löschen einer Anwendung für das IAM Identity Center	Schreiben	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
DisassociateIamRoleFromConnection [nur Berechtigung]	Gewährt die Berechtigung zum Aufheben der Zuordnung einer IAM-Rolle zu einer Verbindung	Schreiben	connections*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateIdentityCenterApplicationFromSpace [nur Berechtigung]	Erteilt die Erlaubnis, eine IAM Identity Center-Anwendung von einem Amazon-Bereich zu trennen CodeCatalyst	Schreiben	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
DisassociateIdentityFromIdentityCenterApplication [nur Berechtigung]	Erteilt die Erlaubnis, eine Identität von einer IAM Identity Center-Anwendung für einen Amazon-Bereich zu trennen CodeCatalyst	Schreiben	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
GetBillingAuthorization [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben der Rechnungsgenehmigungen für eine Verbindung	Lesen	connections*		
				aws:ResourceTag/${TagKey}	
GetConnection [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen einer Verbindung	Lesen	connections*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetIdentityCenterApplication [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Informationen zu einer IAM Identity Center-Anwendung	Lesen	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
GetPendingConnection [nur Berechtigung]	Erteilt die Erlaubnis, eine ausstehende Anfrage zur Verbindung dieses Kontos mit einem CodeCatalyst Amazon-Bereich zu erhalten	Lesen			
ListConnections [nur Berechtigung]	Gewährt die Berechtigung, nicht ausstehende Verbindungen aufzulisten	Auflisten			
ListIamRolesForConnection [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von einer Verbindung zugeordneten IAM-Rollen	Auflisten	connections*		
				aws:ResourceTag/${TagKey}	
ListIdentityCenterApplications [nur Berechtigung]	Gewährt die Berechtigung, eine Liste aller IAM Identity Center-Anwendungen im Konto einzusehen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListIdentityCenterApplicationsForSpace [nur Berechtigung]	Erteilt die Erlaubnis, eine Liste von IAM Identity Center-Anwendungen von Amazon CodeCatalyst Space anzuzeigen	Auflisten			
ListSpacesForIdentityCenterApplication [nur Berechtigung]	Erteilt die Berechtigung, eine Liste von Amazon CodeCatalyst Spaces nach IAM Identity Center-Anwendung anzuzeigen	Auflisten	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource [nur Berechtigung]	Erteilt die Erlaubnis, Tags für eine CodeCatalyst Amazon-Ressource aufzulisten	Lesen	connections		
			identity-center-applications		
				aws:ResourceTag/${TagKey}	
PutBillingAuthorization [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen oder Aktualisieren der Fakturierungsautorisierung für eine Verbindung	Schreiben	connections*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RejectConnection [nur Berechtigung]	Erteilt die Erlaubnis, eine Anfrage zur Verbindung dieses Kontos mit einem CodeCatalyst Amazon-Bereich abzulehnen	Schreiben			
SynchronizeIdentityCenterApplication [nur Berechtigung]	Gewährt die Berechtigung, eine IAM Identity Center-Anwendung mit dem zugrunde liegenden Identitätsspeicher zu synchronisieren	Schreiben	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
TagResource [nur Berechtigung]	Erteilt die Erlaubnis, eine CodeCatalyst Amazon-Ressource zu taggen	Tagging	connections		
			identity-center-applications		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UntagResource [nur Berechtigung]	Erteilt die Erlaubnis, die Markierung einer Amazon-Ressource aufzuheben CodeCatalyst	Tagging	connections		
			identity-center-applications		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateIdentityCenterApplication [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren einer IAM Identity Center-Anwendung	Schreiben	identity-center-applications*		
				aws:ResourceTag/${TagKey}	

Von Amazon definierte Ressourcentypen CodeCatalyst

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
connections	`arn:${Partition}:codecatalyst:${Region}:${Account}:/connections/${ConnectionId}`	aws:ResourceTag/${TagKey}
identity-center-applications	`arn:${Partition}:codecatalyst:${Region}:${Account}:/identity-center-applications/${IdentityCenterApplicationId}`	aws:ResourceTag/${TagKey}
space	`arn:${Partition}:codecatalyst:::space/${SpaceId}`	
project	`arn:${Partition}:codecatalyst:::space/${SpaceId}/project/${ProjectId}`	

Zustandsschlüssel für Amazon CodeCatalyst

Amazon CodeCatalyst definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Schlüssel eines Tags und den Wert einer Anforderung	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	String

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert den Zugriff nach den Tag-Schlüsseln in einer Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS CodeCommit

AWS CodeCommit (Dienstpräfix:`codecommit`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS CodeCommit definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung

mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateApprovalRuleTemplateWithRepository	Gewährt die Berechtigung, eine Genehmigungsregelvorlage einem Repository zuzuordnen.	Write	repository*		
BatchAssociateApprovalRuleT	Gewährt die Berechtigung, eine Genehmigungsregelvorlage mehreren Repositor	Write	repository*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
emplateWithRepositories	ys in einem einzigen Vorgang zuzuordnen.				
BatchDescribeMergeConflicts	Gewährt die Berechtigung zum Abrufen von Informationen über mehrere Zusammenführungskonflikte, wenn Sie versuchen, zwei Commits entweder mit der Dreiwege-Zusammenführungs- oder der Squash-Zusammenführungsoption zusammenzuführen.	Read	repository*		
BatchDisassociateApprovalRuleTemplateFromRepositories	Gewährt die Berechtigung zum Entfernen der Mapping zwischen einer Genehmigungsregelvorlage und mehreren Repositorys in einem einzigen Vorgang.	Schreiben	repository*		
BatchGetCommits	Erteilt die Berechtigung, Informationen über einen oder mehrere Commits in einem Repository zurückzugeben AWS CodeCommit	Lesen	repository*		
BatchGetPullRequests [nur Berechtigung]	Erteilt die Erlaubnis, Informationen über einen oder mehrere Pull-Requests in einem AWS CodeCommit Repository zurückzugeben	Lesen	repository*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetRepositories	Gewährt die Berechtigung zum Abrufen von Informationen über mehrere Repositorys.	Read	repository*		
CancelUploadArchive [nur Berechtigung]	Erteilt die Berechtigung, das Hochladen eines Archivs in eine Pipeline abzubrechen AWS CodePipeline	Lesen	repository*		
CreateApprovalRuleTemplate	Gewährt die Berechtigung zum Erstellen einer Genehmigungsregelvorlage, die automatisch Genehmigungsregeln in Pull-Anforderungen erstellt, die den in der Vorlage definierten Bedingungen entsprechen. Gewährt keine Berechtigung zum Erstellen von Genehmigungsregeln für einzelne Pull-Anforderungen.	Schreiben			
CreateBranch	Erteilt die Erlaubnis, mit dieser API einen Branch in einem AWS CodeCommit Repository zu erstellen; steuert keine Git-Aktionen zum Erstellen von Branches	Schreiben	repository*		
				codecommit:References	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCommit	Erteilt die Berechtigung, einzelne oder mehrere Dateien in einem Branch in einem AWS CodeCommit Repository hinzuzufügen, zu kopieren, zu verschieben oder zu aktualisieren und einen Commit für die Änderungen im angegebenen Branch zu generieren	Schreiben	repository*		
				codecommit:References	
CreatePullRequest	Gewährt die Berechtigung zum Erstellen einer Pull-Anforderung im angegebenen Repository.	Write	repository*		
CreatePullRequestApprovalRule	Gewährt die Berechtigung zum Erstellen einer spezifischen Genehmigungsregel für eine einzelne Pull-Anforderung; Gewährt keine Berechtigung zum Erstellen von Genehmigungsregelvorlagen.	Schreiben	repository*		
CreateRepository	Erteilt die Berechtigung zum Erstellen eines AWS CodeCommit Repositorys	Schreiben	repository*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUnreferencedMergeCommit	Gewährt die Berechtigung zum Erstellen eines unreferenzierten Commits, der das Ergebnis der Zusammenführung von zwei Commits entweder mit der Dreiwege- oder Squash-Zusammenführungsoption enthält; steuert keine Git-Zusammenführungsaktionen.	Write	repository*		
				codecommit:References	
DeleteApprovalRuleTemplate	Gewährt die Berechtigung zum Löschen einer Genehmigungsregelvorlage.	Schreiben			
DeleteBranch	Erteilt die Erlaubnis, einen Branch in einem AWS CodeCommit Repository mit dieser API zu löschen; steuert keine Git-Aktionen zum Löschen von Branches	Schreiben	repository*		
				codecommit:References	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteCommentContent	Gewährt die Berechtigung zum Löschen des Inhalts eines Kommentars zu einer Änderung, einer Datei oder zu einem Commit in einem Repository.	Write	repository*		
DeleteFile	Gewährt die Berechtigung zum Löschen einer angegebenen Datei aus einer bestimmten Verzweigung.	Write	repository*		
				codecommit:References	
DeletePullRequestApprovalRule	Gewährt die Berechtigung zum Löschen einer Genehmigungsregel, die für eine Pull-Anforderung erstellt wurde, wenn die Regel nicht von einer Genehmigungsregelvorlage erstellt wurde.	Schreiben	repository*		
DeleteRepository	Erteilt die Erlaubnis zum Löschen eines AWS CodeCommit Repositorys	Schreiben	repository*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeMergeConflicts	Gewährt die Berechtigung zum Abrufen von Informationen über bestimmte Zusammenführungskonflikte, wenn Sie versuchen, zwei Commits entweder mit der Dreiwege- oder der Squash-Zusammenführungsoption zusammenzuführen.	Read	repository*		
DescribePullRequestEvents	Gewährt die Berechtigung zum Zurückgeben von Informationen zu einem oder mehreren Pull-Anforderungsereignissen.	Read	repository*		
DisassociateApprovalRuleTemplateFromRepository	Gewährt die Berechtigung zum Entfernen der Mapping zwischen einer Genehmigungsregelvorlage und einem Repository.	Write	repository*		
EvaluatePullRequestApprovalRules	Gewährt die Berechtigung zum Auswerten, ob eine Pull-Anforderung basierend auf dem aktuellen Genehmigungsstatus und den Anforderungen der Genehmigungsregeln zusammengeführt werden kann.	Read	repository*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetApprovalRuleTemplate	Gewährt die Berechtigung zum Zurückgeben von Informationen zu einer Genehmigungsregelvorlage.	Lesen			
GetBlob	Erteilt die Berechtigung, den codierten Inhalt einer einzelnen Datei in einem AWS CodeCommit Repository von der AWS CodeCommit Konsole aus anzuzeigen	Lesen	repository*		
GetBranch	Erteilt mit dieser API die Erlaubnis, Details zu einem Branch in einem AWS CodeCommit Repository abzurufen; steuert keine Git-Branch-Aktionen	Lesen	repository*		
GetComment	Gewährt die Berechtigung zum Abrufen des Inhalts eines Kommentars zu einer Änderung, einer Datei oder einem Commit in einem Repository.	Read	repository*		
GetCommentReactions	Gewährt die Berechtigung, die Reaktionen auf einen Kommentar zu erhalten	Read	repository*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetCommentsForComparedCommit	Gewährt die Berechtigung zum Abrufen von Informationen über Kommentare zu einem Vergleich zwischen zwei Commits.	Read	repository*		
GetCommentsForPullRequest	Gewährt die Berechtigung zum Abrufen von Kommentaren zu einer Pull-Anforderung.	Read	repository*		
GetCommit	Gewährt die Berechtigung zum Zurückgeben von Informationen zu einem Commit, einschließlich Commit-Nachricht und Committer-Angaben, mit dieser API; steuert keine Git-Protokollierungsaktionen.	Read	repository*		
GetCommitHistory [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Informationen über den Verlauf von Commits in einem Repository.	Read	repository*		
GetCommitsFromMergeBase [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Informationen über den Unterschied zwischen Commits im Zusammenhang mit einer potenziellen Zusammenführung.	Read	repository*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDifferences	Gewährt die Berechtigung zum Anzeigen von Informationen über die Unterschiede zwischen Commit-Spezifizierern (wie etwa eine Verzweigung, ein Tag, HEAD, eine Commit-ID oder andere vollständig qualifizierte Referenzen).	Read	repository*		
GetFile	Gewährt die Berechtigung zum Zurückgeben des Base-64-kodierten Inhalts einer angegebenen Datei und deren Metadaten.	Read	repository*		
GetFolder	Gewährt die Berechtigung zum Zurückgeben der Inhalte eines angegebenen Ordners in einem Repository.	Read	repository*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetMergeCommit	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Commit für die Zusammenführung mithilfe einer der Zusammenführungsoptionen für Pull-Anforderungen, die Zusammenführungs-Commits erstellt. Nicht alle Zusammenführungsoptionen erstellen Zusammenführungs-Commits. Diese Berechtigung steuert keine Git-Zusammenführungsaktionen.	Read	repository*		
				codecommit:References	
GetMergeConflicts	Gewährt die Berechtigung zum Abrufen von Informationen zu Zusammenführungskonflikten zwischen den „Before“- und „After“-Commit-IDs für eine Pull-Anforderung in einem Repository.	Read	repository*		
GetMergeOptions	Gewährt die Berechtigung zum Abrufen von Informationen über Zusammenführungsoptionen für Pull-Anforderungen, die zum Zusammenführen von zwei Commits verwendet werden können; steuert keine Git-Zusammenführungsaktionen.	Read	repository*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetObjectIdentifier [nur Berechtigung]	Gewährt die Berechtigung zum Auflösen von Blobs, Strukturen und Commits zu ihrem Bezeichner.	Read	repository*		
GetPullRequest	Gewährt die Berechtigung zum Abrufen von Informationen über eine Pull-Anforderung in einem angegebenen Repository.	Read	repository*		
GetPullRequestApprovalStates	Gewährt die Berechtigung zum Abrufen der aktuellen Genehmigungen für eine eingegebene Pull-Anforderung.	Read	repository*		
GetPullRequestOverrideState	Gewährt die Berechtigung, den aktuellen Überschreibungsstatus einer gegebenen Pull-Anforderung abzurufen.	Read	repository*		
GetReferences [nur Berechtigung]	Erteilt die Erlaubnis, Details zu Verweisen in einem AWS CodeCommit Repository abzurufen; steuert keine Git-Referenzaktionen	Lesen	repository*		
GetRepository	Erteilt die Erlaubnis, Informationen über ein AWS CodeCommit Repository abzurufen	Lesen	repository*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetRepositoryTriggers	Gewährt die Berechtigung zum Abrufen von Informationen über Auslöser, die für ein Repository konfiguriert sind.	Read	repository*		
GetTree [nur Berechtigung]	Erteilt die Berechtigung, den Inhalt einer bestimmten Struktur in einem AWS CodeCommit Repository von der AWS CodeCommit Konsole aus anzuzeigen	Lesen	repository*		
GetUploadArchiveStatus [nur Berechtigung]	Erteilt die Berechtigung zum Abrufen von Statusinformationen über einen Archiv-Upload in eine Pipeline in AWS CodePipeline	Lesen	repository*		
GitPull [nur Berechtigung]	Erteilt die Erlaubnis, Informationen aus einem AWS CodeCommit Repository in ein lokales Repository abzurufen	Lesen	repository*		
GitPush [nur Berechtigung]	Erteilt die Erlaubnis, Informationen von einem lokalen Repository in ein Repository zu übertragen AWS CodeCommit	Schreiben	repository*		
				codecommit:References	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListApprovalRuleTemplates	Erteilt die Berechtigung zum Auflisten aller Vorlagen für Genehmigungsregeln in einem AWS-Region für AWS-Konto	Auflisten			
ListAssociatedApprovalRuleTemplatesForRepository	Gewährt die Berechtigung zum Auflisten von Genehmigungsregelvorlagen, die einem Repository zugeordnet sind.	Auflisten	repository*		
ListBranches	Erteilt die Erlaubnis, Branches für ein AWS CodeCommit Repository mit dieser API aufzulisten; steuert keine Git-Branch-Aktionen	Auflisten	repository*		
ListFileCommitHistory	Gewährt die Berechtigung zum Auflisten von Commits und Änderungen an einer angegebenen Datei	Auflisten	repository*		
ListPullRequests	Gewährt die Berechtigung zum Auflisten von Pull-Anforderungen für ein bestimmtes Repository.	Auflisten	repository*		
ListRepositories	Erteilt die Erlaubnis, Informationen über AWS CodeCommit Repositorys in der aktuellen Region für dich aufzulisten AWS-Konto	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListRepositoriesForApprovalRuleTemplate	Gewährt die Berechtigung zum Auflisten von Repositorys, die einer Genehmigungsregelvorlage zugeordnet sind.	Auflisten			
ListTagsForResource	Erteilt die Berechtigung, die an einen Ressourcen-ARN angehängte CodeCommit Ressource aufzulisten	Auflisten	repository		
MergeBranchesByFastForward	Gewährt die Berechtigung zum Zusammenführen von zwei Commits in der angegebene Zielverzweigung unter Verwendung der Fast-Forward-Zusammenführungsoption.	Write	repository*		
				codecommit:References	
MergeBranchesBySquash	Gewährt die Berechtigung zum Zusammenführen von zwei Commits in der angegebenen Zielverzweigung mithilfe der Squash-Zusammenzuführungsoption.	Write	repository*		
				codecommit:References	
MergeBranchesByThreeWay	Gewährt die Berechtigung zum Zusammenführen von zwei Commits in der angegebenen Zielverzweigung mithilfe der Dreiwege-Zusammenführungsoption.	Write	repository*		
				codecommit:References	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
MergePullRequestByFastForward	Gewährt die Berechtigung, eine Pull-Anforderung zu schließen und zu versuchen, sie in der angegebenen Zielverzweigung für diese Pull-Anforderung am angegebenen Commit mithilfe der Fast-Forward-Zusammenführungsoption zusammenzuführen.	Write	repository*		
				codecommit:References	
MergePullRequestBySquash	Gewährt die Berechtigung, eine Pull-Anforderung zu schließen und zu versuchen, sie in der angegebenen Zielverzweigung für diese Pull-Anforderung am angegebenen Commit mithilfe der Squash-Zusammenführungsoption zusammenzuführen.	Write	repository*		
				codecommit:References	
MergePullRequestByThreeWay	Gewährt die Berechtigung, eine Pull-Anforderung zu schließen und zu versuchen, sie in der angegebenen Zielverzweigung für diese Pull-Anforderung am angegebenen Commit mithilfe der Dreiwege-Zusammenführungsoption zusammenzuführen.	Write	repository*		
				codecommit:References	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
OverridePullRequestApprovalRules	Gewährt die Berechtigung, alle Genehmigungsregeln für eine Pull-Anforderung außer Kraft zu setzen, einschließlich Genehmigungsregeln, die von einer Vorlage erstellt wurden.	Write	repository*		
PostCommentForComparedCommit	Gewährt die Berechtigung zum Veröffentlichen eines Kommentars zum Vergleich von zwei Commits.	Write	repository*		
PostCommentForPullRequest	Gewährt die Berechtigung zum Veröffentichen eines Kommentars zu einer Pull-Anforderung.	Write	repository*		
PostCommentReply	Gewährt die Berechtigung zum Posten eines Kommentars als Antwort auf einen Kommentar zu einem Vergleich zwischen Commits oder zu einer Pull-Anforderung.	Write	repository*		
PutCommentReaction	Gewährt die Berechtigung, eine Reaktion auf einen Kommentar zu posten	Schreiben	repository*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutFile	Erteilt die Berechtigung, eine Datei in einem Branch in einem AWS CodeCommit Repository hinzuzufügen oder zu aktualisieren und einen Commit für die Hinzufügung im angegebenen Branch zu generieren	Schreiben	repository*		
				codecommit:References	
PutRepositoryTriggers	Gewährt die Berechtigung zum Erstellen, Aktualisieren oder Löschen von Auslösern für ein Repository.	Schreiben	repository*		
TagResource	Erteilt die Berechtigung, Ressourcen-Tags an einen CodeCommit Ressourcen-ARN anzuhängen	Tagging	repository		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TestRepositoryTriggers	Gewährt die Berechtigung zum Testen der Funktionsfähigkeit von Repository-Auslösern, indem Daten an das Auslöserziel gesendet werden.	Schreiben	repository*		
UntagResource	Erteilt die Berechtigung, Ressourcen-Tags von einem CodeCommit Ressourcen-ARN zu trennen	Tagging	repository		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateApprovalRuleTemplateContent	Gewährt die Berechtigung zum Aktualisieren des Inhalts von Genehmigungsregelvorlagen; Gewährt keine Berechtigung zum Aktualisieren von Inhalten von Genehmigungsregeln, die speziell für Pull-Anforderungen erstellt wurden.	Write			
UpdateApprovalRuleTemplateDescription	Gewährt die Berechtigung zum Aktualisieren der Beschreibung von Genehmigungsregelvorlagen.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateApprovalRuleTemplateName	Gewährt die Berechtigung zum Aktualisieren des Namens von Genehmigungsregelvorlagen.	Write			
UpdateComment	Gewährt die Berechtigung zum Aktualisieren des Inhalts eines Kommentars, wenn die Identität der Identität entspricht, mit der der Kommentar erstellt wurde.	Schreiben	repository*		
UpdateDefaultBranch	Erteilt die Berechtigung, den Standardzweig in einem AWS CodeCommit Repository zu ändern	Schreiben	repository*		
UpdatePullRequestApprovalRuleContent	Gewährt die Berechtigung zum Aktualisieren des Inhalts für Genehmigungsregeln, die für bestimmte Pull-Anforderungen erstellt wurden; Gewährt keine Berechtigung zum Aktualisieren von Genehmigungsregelinhalten für Regeln, die mit einer Genehmigungsregelvorlage erstellt wurden.	Write	repository*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdatePullRequestApprovalState	Gewährt die Berechtigung zum Aktualisieren des Genehmigungsstatus für Pull-Anforderungen	Write	repository*		
UpdatePullRequestDescription	Gewährt die Berechtigung zum Aktualisieren der Beschreibung einer Pull-Anforderung.	Write	repository*		
UpdatePullRequestStatus	Gewährt die Berechtigung zum Aktualisieren des Status einer Pull-Anforderung.	Write	repository*		
UpdatePullRequestTitle	Gewährt die Berechtigung zum Aktualisieren des Titels einer Pull-Anforderung.	Schreiben	repository*		
UpdateRepositoryDescription	Erteilt die Berechtigung, die Beschreibung eines AWS CodeCommit Repositorys zu ändern	Schreiben	repository*		
UpdateRepositoryEncryptionKey	Erteilt die Berechtigung zum Ändern des AWS KMS-Verschlüsselungsschlüssels, der zum Verschlüsseln und Entschlüsseln eines Repositorys verwendet wird AWS CodeCommit	Schreiben	repository*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateRepositoryName	Erteilt die Berechtigung, den Namen eines Repositorys zu ändern AWS CodeCommit	Schreiben	repository*		
UploadArchive [nur Berechtigung]	Erteilt der Servicerolle die Berechtigung AWS CodePipeline , Repository-Änderungen in eine Pipeline hochzuladen	Schreiben	repository*		

Von AWS CodeCommit definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
repository	`arn:${Partition}:codecommit:${Region}:${Account}:${RepositoryName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS CodeCommit

AWS CodeCommit definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	String
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString
codecommit:References	Filtert den Zugriff per Git-Referenz auf angegebene AWS CodeCommit Aktionen	String

Aktionen, Ressourcen und Bedingungsschlüssel für AWS CodeConnections

AWS CodeConnections (Dienstpräfix:`codeconnections`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS CodeConnections definierte Aktionen
- Von AWS CodeConnections definierte Ressourcentypen
- Bedingungsschlüssel für AWS CodeConnections

Von AWS CodeConnections definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateConnection	Gewährt die Berechtigung zum Erstellen einer Verbindungsressource.	Write		aws:RequestTag/${TagKey} aws:TagKeys codeconnections:ProviderType	
CreateHost	Gewährt die Berechtigung zum Erstellen einer Host-Ressource	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys codeconnections:ProviderType	
CreateRepositoryLink	Gewährt die Berechtigung zum Erstellen eines Repository-Links	Schreiben	Connection*		codeconnections:PassConnection codeconnections:UseConnection

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSyncConfiguration	Gewährt die Berechtigung zum Erstellen einer Vorlage für die Sync-Konfiguration	Schreiben	RepositoryLink*		codeconnections:PassRepository iam:PassRole
				codeconnections:Branch	
DeleteConnection	Gewährt die Berechtigung zum Löschen einer Verbindungsressource.	Write	Connection*		
DeleteHost	Gewährt die Berechtigung zum Löschen einer Host-Ressource	Schreiben	Host*		
DeleteRepositoryLink	Gewährt die Berechtigung zum Löschen eines Repository-Links	Schreiben	RepositoryLink*		
DeleteSyncConfiguration	Gewährt die Berechtigung zum Löschen einer Synchronisierungskonfiguration	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetConnection	Gewährt die Berechtigung zum Abrufen von Details zu einer Verbindungsressource.	Read	Connection*		
GetHost	Gewährt die Berechtigung zum Abrufen von Details über eine Host-Ressource	Read	Host*		
GetIndividualAccessToken [nur Berechtigung]	Gewährt die Berechtigung, einen Drittanbieter, z. B. eine Bitbucket-App-Installation, mit einer Verbindung zu verknüpfen	Read		codeconnections:ProviderType	codeconnections:StartOAuthHandshake
GetInstallationUrl [nur Berechtigung]	Gewährt die Berechtigung, einen Drittanbieter, z. B. eine Bitbucket-App-Installation, mit einer Verbindung zu verknüpfen	Lesen		codeconnections:ProviderType	
GetRepositoryLink	Gewährt die Berechtigung zum Beschreiben eines Repository-Links	Lesen	RepositoryLink*		
GetRepositorySyncStatus	Gewährt die Berechtigung zum Abrufen des neuesten Synchronisierungsstatus für ein Repository	Lesen	RepositoryLink*		
				codeconnections:Branch	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetResourceSyncStatus	Gewährt die Berechtigung zum Abrufen des neuesten Synchronisierungsstatus für eine Ressource (CFN-Stack oder andere Ressourcen)	Lesen			
GetSyncBlockerSummary	Gewährt die Berechtigung zum Beschreiben von Service-Synchronisierungssperren für eine Ressource (CFN-Stack oder andere Ressourcen)	Lesen			
GetSyncConfiguration	Gewährt die Berechtigung, eine Synchronisierungskonfiguration zu beschreiben	Lesen			
ListConnections	Gewährt die Berechtigung zum Auflisten von Verbindungsressourcen.	List	Connection*		
				codeconnections:ProviderTypeFilter	
ListHosts	Gewährt die Berechtigung zum Auflisten von Host-Ressourcen	List		codeconnections:ProviderTypeFilter	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListInstallationTargets [nur Berechtigung]	Gewährt die Berechtigung, einen Drittanbieter, z. B. eine Bitbucket-App-Installation, mit einer Verbindung zu verknüpfen	Auflisten			codeconnections:GetIndividualAccessToken codeconnections:StartOAuthHandshake
ListRepositoryLinks	Gewährt die Berechtigung zum Auflisten von Repository-Links	Auflisten			
ListRepositorySyncDefinitions	Gewährt die Berechtigung zum Auflisten von Sync-Definitionen	Auflisten			
ListSyncConfigurations	Gewährt die Berechtigung zum Auflisten der Synchronisierungskonfigurationen für einen Repository-Link	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Abrufen von Schlüssel-Wert-Paaren, die verwendet werden, um die Ressource zu verwalten.	Auflisten	Connection		
			Host		
			RepositoryLink		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PassConnection [nur Berechtigung]	Erteilt die Berechtigung, eine Verbindungsressource an einen AWS Dienst zu übergeben, der einen Verbindungs-ARN als Eingabe akzeptiert, z. B. codepipeline: CreatePipeline	Lesen	Connection*		
				codeconnections:PassedToService	
PassRepository [nur Berechtigung]	Erteilt die Berechtigung, eine Repository-Link-Ressource an einen AWS Dienst zu übergeben, der a RepositoryLinkId als Eingabe akzeptiert, z. B. codeconnections: CreateSyncConfiguration	Lesen	RepositoryLink*		
				codeconnections:PassedToService	
RegisterAppCode [nur Berechtigung]	Erteilt die Berechtigung, einen Server eines Drittanbieters, z. B. eine GitHub Enterprise Server-Instanz, einem Host zuzuordnen	Lesen		codeconnections:HostArn	
StartAppRegistrationHandshake [nur Berechtigung]	Erteilt die Berechtigung, einen Server eines Drittanbieters, z. B. eine GitHub Enterprise Server-Instanz, einem Host zuzuordnen	Lesen		codeconnections:HostArn	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartOAuthHandshake [nur Berechtigung]	Gewährt die Berechtigung, einen Drittanbieter, z. B. eine Bitbucket-App-Installation, mit einer Verbindung zu verknüpfen	Lesen		codeconnections:ProviderType	
TagResource	Gewährt die Berechtigung zum Hinzufügen oder Ändern der Tags zur angegebenen Ressource	Tagging	Connection		
			Host		
			RepositoryLink		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Erteilt die Berechtigung, Tags aus einer AWS Ressource zu entfernen	Tagging	Connection		
			Host		
			RepositoryLink		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateConnectionInstallation	Erteilt die Berechtigung, eine Verbindungsressource mit einer Installation der CodeStar Connections-App zu aktualisieren	Schreiben	Connection*		codeconnections:GetIndividualAccessToken codeconnections:GetInstallationUrl codeconnections:ListInstallationTargets codeconnections:StartOAuthHandshake
				codeconnections:InstallationId	
UpdateHost	Gewährt die Berechtigung zum Aktualisieren einer Hostressource	Schreiben	Host*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateRepositoryLink	Gewährt die Berechtigung zum Aktualisieren eines Repository-Links	Schreiben	RepositoryLink*		
UpdateSyncBlocker	Gewährt die Berechtigung, einen Synchronisierungs-Blocker für eine Ressource (CFN-Stack oder andere Ressourcen) zu aktualisieren	Schreiben			
UpdateSyncConfiguration	Gewährt die Berechtigung zum Aktualisieren einer Synchronisierungskonfiguration.	Schreiben		codeconnections:Branch	
UseConnection [nur Berechtigung]	Gewährt die Berechtigung, eine Verbindungsressource zum Aufrufen von Anbieteraktionen zu verwenden	Lesen	Connection*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				codeconnections:BranchName codeconnections:FullRepositoryId codeconnections:OwnerId codeconnections:ProviderAction codeconnections:ProviderPermissionsRequired codeconnections:RepositoryName	

Von AWS CodeConnections definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der

Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Connection	`arn:${Partition}:codeconnections:${Region}:${Account}:connection/${ConnectionId}`	aws:ResourceTag/${TagKey}
Host	`arn:${Partition}:codeconnections:${Region}:${Account}:host/${HostId}`	aws:ResourceTag/${TagKey}
RepositoryLink	`arn:${Partition}:codeconnections:${Region}:${Account}:repository-link/${RepositoryLinkId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS CodeConnections

AWS CodeConnections definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString
codeconnections:Branch	Filtert den Zugriff nach dem Zweignamen, der in der Anforderung übergeben wird	String
codeconnections:BranchName	Filtert den Zugriff nach dem Zweignamen, der in der Anforderung übergeben wird. Gilt nur für UseConnection Anfragen nach Zugriff auf einen bestimmten Repository-Zweig	String
codeconnections:FullRepositoryId	Filtert den Zugriff durch das Repository, das in der Anforderung übergeben wird. Gilt nur für UseConnection Anfragen nach Zugriff auf ein bestimmtes Repository	String
codeconnections:HostArn	Filtert den Zugriff durch die Host-Ressource, die mit der in der Anforderung verwendeten Verbindung verknüpft ist	ARN
codeconnections:InstallationId	Filtert den Zugriff nach der Drittanbieter-ID (z. B. der Bitbucket-App-Installations-ID für CodeConnections), die zur Aktualisierung einer Verbindung verwendet wird. Ermöglicht Ihnen, einzuschränken, welche App-Installationen von Drittanbietern zum Herstellen einer Verbindung verwendet werden können.	Zeichenfolge
codeconnections:OwnerId	Filtert den Zugriff durch den Eigentümer des Drittanbieter-Repositorys. Gilt nur für UseConnection Anfragen nach Zugriff auf Repositorys, die einem bestimmten Benutzer gehören	String

Bedingungsschlüssel	Beschreibung	Typ
codeconnections:PassedToService	Filtert den Zugriff nach dem Dienst, an den der Principal eine Verbindung übergeben darf, oder RepositoryLink	String
codeconnections:ProviderAction	Filtert den Zugriff nach der Provider-Aktion in einer UseConnection Anfrage wie ListRepositories. Alle gültigen Werte finden Sie in der Dokumentation.	ArrayOfString
codeconnections:ProviderPermissionsRequired	Filtert den Zugriff anhand der Schreibberechtigungen einer Anbieteraktion in einer UseConnection Anfrage. Gültige Typen umfassen read_only und read_write.	Zeichenfolge
codeconnections:ProviderType	Filtert den Zugriff nach dem Typ des Drittanbieters, der in der Anforderung übergeben wurde.	Zeichenfolge
codeconnections:ProviderTypeFilter	Filtert den Zugriff nach dem Typ des Drittanbieters, der zum Filtern der Ergebnisse verwendet wird.	Zeichenfolge
codeconnections:RepositoryName	Filtert den Zugriff nach dem Repository-Namen, der in der Anforderung übergeben wird. Gilt nur für UseConnection Anfragen nach Zugriff auf Repositorys, die einem bestimmten Benutzer gehören	String

Aktionen, Ressourcen und Bedingungsschlüssel für AWS CodeDeploy

AWS CodeDeploy (Servicepräfix: `codedeploy`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.

- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS CodeDeploy definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddTagsToOnPremisesInstances	Erteilt die Berechtigung zum Hinzufügen von Tags zu einer oder mehreren On-Premises Instances	Markierung	instance*		
BatchGetApplicationRevisions	Gewährt die Berechtigung zum Abrufen von Informationen zu einer oder mehreren Anwendungsrevisionen	Lesen	application*		
BatchGetApplications	Gewährt die Berechtigung zum Abrufen von Informationen zu mehreren Anwendungen, die dem IAM-Benutzer zugeordnet sind	Lesen	application*		
BatchGetDeploymentGroups	Gewährt die Berechtigung zum Abrufen von Informationen zu einzelnen oder mehreren Bereitstellungsgruppen	Lesen	deploymentgroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetDeploymentInstances	Gewährt die Berechtigung zum Abrufen Informationen über eine oder mehrere Instances, die Teil einer Bereitstellungsgruppe sind	Lesen	deploymentgroup*		
BatchGetDeploymentTargets	Gewährt die Berechtigung zum Zurückgeben eines Arrays mit einem oder mehreren Zielen, die mit einer Bereitstellung verknüpft sind. Diese Methode funktioniert mit allen Compute-Typen und sollte anstelle der veralteten BatchGetDeploymentInstances verwendet werden. Die maximale Anzahl der Ziele, die zurückgegeben werden können, ist 25	Lesen			
BatchGetDeployments	Gewährt die Berechtigung zum Abrufen von Informationen zu mehreren Bereitstellungen, die dem IAM-Benutzer zugeordnet sind	Lesen	deploymentgroup*		
BatchGetOnPremisesInstances	Gewährt die Berechtigung zum Abrufen von Informationen über eine oder mehrere On-Premises Instances	Lesen	instance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ContinueDeployment	Erteilt die Berechtigung zum Starten des Prozesses der Umleitung des Datenverkehrs von Instances in der ursprünglichen Umgebung zu Instances in der Platzierungsumgebung, ohne die angegebene Wartezeit verstreichen zu lassen	Schreiben			
CreateApplication	Gewährt die Berechtigung zum Erstellen einer Anwendung, die dem IAM-Benutzer zugeordnet ist	Schreiben	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudFormationDeployment [nur Berechtigung]	Erteilt die Berechtigung zum Erstellen der CloudFormation-Bereitstellung zur Orchestrierung eines CloudFormation-Stack-Updates	Schreiben			
CreateDeployment	Gewährt die Berechtigung zum Erstellen einer Bereitstellung für eine Anwendung, die dem IAM-Benutzer zugeordnet ist	Schreiben	deploymentgroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDeploymentConfig	Erteilt die Berechtigung zum Erstellen einer benutzerdefinierten Bereitstellungskonfiguration, die dem IAM-Benutzer zugeordnet ist	Schreiben	deploymentconfig*		
CreateDeploymentGroup	Gewährt die Berechtigung zum Erstellen einer Bereitstellungsgruppe für eine Anwendung, die dem IAM-Benutzer zugeordnet ist	Schreiben	deploymentgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Gewährt die Berechtigung zum Löschen einer Anwendung, die dem IAM-Benutzer zugeordnet ist	Schreiben	application*		
DeleteDeploymentConfig	Erteilt die Berechtigung zum Löschen einer benutzerdefinierten Bereitstellungskonfiguration, die dem IAM-Benutzer zugeordnet ist	Schreiben	deploymentconfig*		
DeleteDeploymentGroup	Gewährt die Berechtigung zum Löschen einer Bereitstellungsgruppe für eine Anwendung, die dem IAM-Benutzer zugeordnet ist	Schreiben	deploymentgroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteGitHubAccountToken	Gewährt die Berechtigung zum Löschen einer GitHub-Kontoverbindung	Schreiben			
DeleteResourcesByExternalId	Erteilt die Berechtigung zum Löschen von Ressourcen, die mit der angegebenen externen ID verknüpft sind	Schreiben			
DeregisterOnPremisesInstance	Gewährt die Berechtigung zum Aufheben der Registrierung einer On-Premises Instance	Schreiben	instance*		
GetApplication	Gewährt die Berechtigung zum Aufheben von Informationen zu einer dem IAM-Benutzer zugeordneten Anwendung	Auflisten	application*		
GetApplicationRevision	Erteilt die Berechtigung zum Abrufen von Informationen zu einer Anwendungsrevision für eine dem IAM-Benutzer zugeordnete Anwendung	Auflisten	application*		
GetDeployment	Gewährt die Berechtigung zum Abrufen von Informationen über eine einzelne Bereitstellung für eine Bereitstellungsgruppe einer dem IAM-Benutzer zugeordneten Anwendung	Auflisten	deploymentgroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDeploymentConfig	Gewährt die Berechtigung zum Abrufen von Informationen zu einer einzelnen, dem IAM-Benutzer zugeordneten Bereitstellungskonfiguration	Auflisten	deploymentconfig*		
GetDeploymentGroup	Erteilt die Berechtigung zum Abrufen von Informationen zu einer einzelnen Bereitstellungsgruppe für eine dem IAM-Benutzer zugeordnete Anwendung	Auflisten	deploymentgroup*		
GetDeploymentInstance	Gewährt die Berechtigung zum Abrufen von Informationen zu einer einzelnen Instance in einer dem IAM-Benutzer zugeordneten Bereitstellung	Auflisten	deploymentgroup*		
GetDeploymentTarget	Gewährt die Berechtigung zum Abrufen von Informationen über ein Bereitstellungsziel	Lesen			
GetOnPremisesInstance	Gewährt die Berechtigung zum Abrufen von Informationen über eine On-Premises Instance	Auflisten	instance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListApplicationRevisions	Erteilt die Berechtigung zum Abrufen von Informationen zu allen Anwendungsrevisionen für eine dem IAM-Benutzer zugeordnete Anwendung	Auflisten	application*		
ListApplications	Gewährt die Berechtigung zum Abrufen von Informationen zu allen Anwendungen, die dem IAM-Benutzer zugeordnet sind	Auflisten			
ListDeploymentConfigs	Gewährt die Berechtigung zum Abrufen von Informationen zu allen dem IAM-Benutzer zugeordneten Bereitstellungskonfiguration	Auflisten			
ListDeploymentGroups	Erteilt die Berechtigung zum Ändern von Informationen zu allen Bereitstellungsgruppen für eine dem IAM-Benutzer zugeordnete Anwendung	Auflisten	application*		
ListDeploymentInstances	Gewährt die Berechtigung zum Abrufen von Informationen zu allen Instances in einer dem IAM-Benutzer zugeordneten Bereitstellung	Auflisten	deploymentgroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDeploymentTargets	Gewährt die Berechtigung zum Zurückgeben eines Arrays mit Ziel-IDs, die einer Bereitstellung zugeordnet sind	Auflisten			
ListDeployments	Gewährt die Berechtigung zum Abrufen von Informationen zu allen Bereitstellungen in einer dem IAM-Benutzer zugeordneten Bereitstellungsgruppe oder alle dem IAM-Benutzer zugeordneten Bereitstellungen	Auflisten	deploymentgroup*		
ListGitHubAccountTokenNames	Gewährt die Berechtigung zum Auflisten der Namen der gespeicherten Verbindungen zu GitHub-Konten	Auflisten			
ListOnPremisesInstances	Gewährt die Berechtigung zum Auflisten mit einem oder mehreren On-Premises Instance-Namen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Zurückgeben einer Liste von Tags für die Ressource, die durch einen angegebenen ARN identifiziert wird. Tags werden verwendet, um Ihre CodeDeploy-Ressourcen zu organisieren und zu kategorisieren	Auflisten	application		
			deploymentgroup		
PutLifecycleEventHookExecutionStatus	Gewährt die Berechtigung zum Benachrichtigen des Ausführungsstatus eines Lebenszyklusereignis-Hooks für eine dem IAM-Benutzer zugeordnete Bereitstellung	Schreiben			
RegisterApplicationRevision	Gewährt die Berechtigung zum Registrieren von Informationen über eine Anwendungsrevision für eine dem IAM-Benutzer zugeordnete Anwendung	Schreiben	application*		
RegisterOnPremisesInstance	Gewährt die Berechtigung zum Registrieren einer On-Premises Instance	Schreiben	instance*		
RemoveTagsFromOnPremisesInstances	Erteilt die Berechtigung zum Entfernen von Tags von einer oder mehreren On-Premises Instances	Markierung	instance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SkipWaitTimeForInstanceTermination	Gewährt die Berechtigung zum Überschreiben jeder angegebenen Wartezeit und beginnt mit dem Beenden von Instances unmittelbar nach Abschluss des Traffic-Routings. Diese Aktion gilt nur für Blau/Grün-Bereitstellungen	Schreiben			
StopDeployment	Gewährt die Berechtigung zum Beenden einer Bereitstellung	Schreiben			
TagResource	Gewährt die Berechtigung zum Zuordnen der Liste der Tags im Input-Tags-Parameter der Ressource, die durch den ResourceArn-Eingangsparameter identifiziert wird	Markierung	application		
			deploymentgroup		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UntagResource	Erteilt die Berechtigung zum Aufheben der Zuordnung einer Ressource zu einer Liste von Tags. Die Ressource wird durch den Eingangsparameter ResourceArn identifiziert. Die Tags werden durch die Liste der Schlüssel im Eingangsparameter TagKeys identifiziert	Markierung	application		
			deploymentgroup		
				aws:TagKeys	
UpdateApplication	Gewährt die Berechtigung zum Aktualisieren einer Anwendung	Schreiben	application*		
UpdateDeploymentGroup	Erteilt die Berechtigung zum Ändern von Informationen zu einer einzelnen Bereitstellungsgruppe für eine dem IAM-Benutzer zugeordnete Anwendung	Schreiben	deploymentgroup*		

Von AWS CodeDeploy definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
application	`arn:${Partition}:codedeploy:${Region}:${Account}:application:${ApplicationName}`	
deploymentconfig	`arn:${Partition}:codedeploy:${Region}:${Account}:deploymentconfig:${DeploymentConfigurationName}`	
deploymentgroup	`arn:${Partition}:codedeploy:${Region}:${Account}:deploymentgroup:${ApplicationName}/${DeploymentGroupName}`	
instance	`arn:${Partition}:codedeploy:${Region}:${Account}:instance:${InstanceName}`	

Bedingungsschlüssel für AWS CodeDeploy

AWS CodeDeploy definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung.	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf den Tag-Schlüssel-Wert-Paaren, die an die Ressource angefügt wurden.	Zeichenfolge
aws:TagKeys	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für sichere Host-Befehle mit dem AWS-CodeDeploy-Service

Der Service für sichere Host-Befehle, AWS-CodeDeploy, (Servicepräfix: `codedeploy-commands-secure`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Vom Service für sichere Host-Befehle, AWS CodeDeploy, definierte Aktionen
- Ressourcen-Typen, die vom Service für sichere Host-Befehle, AWS CodeDeploy, definiert werden
- Bedingungsschlüssel für sichere Host-Befehle mit dem AWS-CodeDeploy-Service

Vom Service für sichere Host-Befehle, AWS CodeDeploy, definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDeploymentSpecification	Gewährt die Berechtigung zum Abrufen von Bereitstellungsdetails	Lesen			
PollHostCommand	Gewährt die Berechtigung zum Anfordern von Host-Agent-Befehlen	Lesen			
PutHostCommandAcknowledgement	Gewährt die Berechtigung zum Kennzeichnen von Host-Agent-Befehlen	Schreiben			
PutHostCommandComplete	Gewährt die Berechtigung zum Kennzeichnen von Host-Agent-Befehlen	Schreiben			

Ressourcen-Typen, die vom Service für sichere Host-Befehle, AWS CodeDeploy, definiert werden

Der Service für sichere Host-Befehle, AWS CodeDeploy unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Geben Sie `"Resource": "*"` in Ihrer Richtlinie an, um Zugriff auf den Service für sichere Host-Befehle, AWS CodeDeploy, zu gewähren.

Bedingungsschlüssel für sichere Host-Befehle mit dem AWS-CodeDeploy-Service

CodeDeploy Commands Secure besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CodeGuru

Amazon CodeGuru (Servicepräfix: `codeguru`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon CodeGuru definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetCodeGuruFreeTrialSummary [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen einer Free-Trial-Übersicht für den CodeGuru-Service, die das Ablaufdatum enthält	Lesen			

Von Amazon CodeGuru definierte Ressourcentypen

Amazon CodeGuru unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf Amazon CodeGuru zu erlauben, geben Sie in Ihrer Richtlinie `"Resource": "*"` an.

Bedingungsschlüssel für Amazon CodeGuru

CodeGuru besitzt keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CodeGuru Profiler

Amazon CodeGuru Profiler (Service-Präfix: `codeguru-profiler`) bietet die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontext-Schlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon CodeGuru Profiler definierte Aktionen
- Von Amazon CodeGuru Profiler definierte Ressourcentypen
- Bedingungsschlüssel für Amazon CodeGuru Profiler

Von Amazon CodeGuru Profiler definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt,

müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddNotificationChannels	Gewährt die Berechtigung zum Hinzufügen von bis zu 2 Themen-ARNs vorhandener AWS-SNS-Themen zum Veröffentlichen von Benachrichtigungen	Schreiben	Profiling Group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetFrameMetricData	Gewährt die Berechtigung zum Abrufen der Frame-Metrikdaten für eine Profiling-Gruppe	Auflisten	Profiling Group*		
ConfigureAgent	Gewährt die Berechtigung zum Registrieren beim Orchestrierungsservice und zum Abrufen von Profilkonfigurationsinformationen, die von Kundendienstmitarbeitern verwendet werden	Schreiben	Profiling Group*		
CreateProfilingGroup	Gewährt die Berechtigung zum Erstellen einer Profilerstellungsgruppe	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteProfilingGroup	Gewährt die Berechtigung zum Löschen einer Profilerstellungsgruppe	Schreiben	Profiling Group*		
DescribeProfilingGroup	Gewährt die Berechtigung zum Beschreiben einer Profilerstellungsgruppe	Read	Profiling Group*		
GetFindingsReportAccountSummary	Gewährt die Berechtigung, eine Zusammenfassung der letzten Empfehlungen für jede Profilerstellungsgruppe im Konto abzurufen	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetNotificationConfiguration	Gewährt die Berechtigung zum Abrufen der Benachrichtigungskonfiguration	Lesen	Profiling Group*		
GetPolicy	Gewährt die Berechtigung zum Abrufen der Ressourcenrichtlinie, die der angegebenen Profilerstellungsgruppe zugeordnet ist	Lesen	Profiling Group*		
GetProfile	Gewährt die Berechtigung zum Abrufen aggregierter Profile für eine bestimmte Profilerstellungsgruppe	Read	Profiling Group*		
GetRecommendations	Gewährt die Berechtigung zum Abrufen von Empfehlungen.	Read	Profiling Group*		
ListFindingsReports	Gewährt Berechtigungen zum Auflisten der verfügbaren Empfehlungsberichte für eine bestimmte Profiling-Gruppe	List	Profiling Group*		
ListProfileTimes	Gewährt Berechtigungen zum Auflisten der Startzeiten der verfügbaren aggregierten Profile für eine bestimmte Profiling-Gruppe	List	Profiling Group*		
ListProfilingGroups	Gewährt Berechtigungen zum Auflisten von Profiling-Gruppen im Konto	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Profiling-Gruppe	Auflisten	Profiling Group*		
PostAgentProfile	Gewährt Berechtigungen zum Senden eines Profils, das von einem Agenten, der zu einer bestimmten Profiling-Gruppe gehört, zur Aggregation erfasst wurde	Schreiben	Profiling Group*		
PutPermission	Gewährt die Berechtigung zum Aktualisieren der Liste der Prinzipale, die für eine Aktionsgruppe in der Ressourcenrichtlinie zulässig sind, die der angegebenen Profiling-Gruppe zugeordnet ist	Berechtigungsverwaltung	Profiling Group*		
RemoveNotificationChannel	Gewährt die Berechtigung zum Löschen eines bereits konfigurierten SNStopic-ARN aus der Benachrichtigungskonfiguration	Schreiben	Profiling Group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RemovePermission	Gewährt die Berechtigung zum Entfernen der Berechtigung der angegebenen Aktionsgruppe aus der Ressourcenrichtlinie, die der angegebenen Profilerstellungsgruppe zugeordnet ist	Berechtigungsverwaltung	Profiling Group*		
SubmitFeedback	Gewährt die Berechtigung, Benutzer-Feedback für nützliche oder nicht nützliche Anomalien einzureichen	Schreiben	Profiling Group*		
TagResource	Gewährt die Berechtigung zum Hinzufügen oder Überschreiben von Tags zu einer Profiling-Gruppe	Markieren	Profiling Group*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Profiling-Gruppe	Markieren	Profiling Group*		
				aws:TagKeys	
UpdateProfilingGroup	Gewährt die Berechtigung zum Aktualisieren einer bestimmten Profiling-Gruppe	Schreiben	Profiling Group*		

Von Amazon CodeGuru Profiler definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Profiling Group	`arn:${Partition}:codeguru-profiler:${Region}:${Account}:profilingGroup/${ProfilingGroupName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon CodeGuru Profiler

Amazon CodeGuru Profiler definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CodeGuru Reviewer

Amazon CodeGuru Reviewer (Service-Präfix: `codeguru-reviewer`) bietet die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontext-Schlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon CodeGuru Reviewer definierte Aktionen
- Von Amazon CodeGuru Reviewer definierte Ressourcentypen
- Bedingungsschlüssel für Amazon CodeGuru Reviewer

Von Amazon CodeGuru Reviewer definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Associate Repository	Gewährt die Berechtigung, ein Repository mit Amazon CodeGuru Reviewer zu verknüpfen.	Schreiben		aws:RequestTag/${TagKey}	codecommit:GetRepository

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	codecommit:ListRepositories codecommit:TagResource codestar-connections:PassConnection events:PutRule events:PutTargets iam:CreateServiceLinkedRole s3:CreateBucket s3:ListBucket s3:PutBucketPolicy

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					s3:PutLifecycleConfiguration
CreateCodeReview	Gewährt die Berechtigung zum Erstellen einer Codeüberprüfung	Schreiben	association*		s3:GetObject
				aws:ResourceTag/${TagKey}	
CreateConnectionToken [nur Berechtigung]	Gewährt die Berechtigung, einen webbasierten oauth-Handshake für Drittanbieter durchzuführen.	Read			
DescribeCodeReview	Gewährt die Berechtigung zur Beschreibung einer Codeüberprüfung	Read	association*		
				aws:ResourceTag/${TagKey}	
DescribeRecommendationFeedback	Gewährt die Berechtigung, ein Empfehlungsfeedback zu einer Codeüberprüfung zu beschreiben	Read	association*		
				aws:ResourceTag/${TagKey}	
DescribeRepositoryAssociation	Gewährt die Berechtigung zum Beschreiben einer Repository-Mapping	Read	association*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
DisassociateRepository	Gewährt die Berechtigung, ein Repository mit Amazon CodeGuru Reviewer zu trennen	Schreiben	association*		codecommit:UntagResource events:DeleteRule events:RemoveTargets
				aws:ResourceTag/${TagKey}	
GetMetricsData [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen von Pull-Anforderungsmetriken in der Konsole	Read			
ListCodeReviews	Gewährt die Berechtigung, eine Zusammenfassung der Codeüberprüfung aufzulisten.	List			
ListRecommendationFeedback	Gewährt die Berechtigung, eine Zusammenfassung des Empfehlungs-Feedbacks zu einer Codeüberprüfung aufzulisten	List	association*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListRecommendations	Gewährt die Berechtigung, eine Zusammenfassung der Empfehlungen für eine Codeüberprüfung aufzulisten.	List	association*		
				aws:ResourceTag/${TagKey}	
ListRepositoryAssociations	Gewährt die Berechtigung zum Auflisten einer Zusammenfassung der Repository-Mappings	List			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Ressource, die einem Repository-ARN angefügt ist	List	association*		
				aws:ResourceTag/${TagKey}	
ListThirdPartyRepositories [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der Repositorys von Drittanbietern in der Konsole	Read			
PutRecommendationFeedback	Gewährt die Berechtigung, Feedback für eine Empfehlung zu einer Codeüberprüfung abzugeben	Schreiben	association*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Anhängen von Ressourcen-Tags an einen zugeordneten Repository-ARN	Markieren	association*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UnTagResource	Gewährt die Berechtigung zum Trennen von Ressourcen-Tags von einem zugeordneten Repository-ARN	Markieren	association*		
				aws:TagKeys	

Von Amazon CodeGuru Reviewer definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
association	`arn:${Partition}:codeguru-reviewer:${Region}:${Account}:association:${ResourceId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
codereview	`arn:${Partition}:codeguru-reviewer:${Region}:${Account}:association:${ResourceId}:codereview:${CodeReviewId}`	

Bedingungsschlüssel für Amazon CodeGuru Reviewer

Amazon CodeGuru Reviewer definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Zugriff basierend auf dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung.	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf den Tag-Schlüssel-Wert-Paaren, die an die Ressource angefügt wurden.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf dem Vorhandensein von Tag-Schlüsseln in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CodeGuru Security

Amazon CodeGuru Security (Servicepräfix: `codeguru-security`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon CodeGuru Security definierte Aktionen
- Von Amazon CodeGuru Security definierte Ressourcentypen
- Bedingungsschlüssel für Amazon CodeGuru Security

Von Amazon CodeGuru Security definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetFindings	Gewährt die Berechtigung zum Batch-Abrufen bestimmter von CodeGuru Security generierter Ergebnisse	Lesen	ScanName		
CreateScan	Gewährt die Berechtigung zum Erstellen eines CodeGuru-Security-Scans	Schreiben	ScanName		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateUploadUrl	Gewährt die Berechtigung zum Generieren einer vorsignierten URL zum Hochladen von Codearchiven	Schreiben	ScanName		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteScansByCategory [nur Berechtigung]	Gewährt die Berechtigung zum Löschen aller Scans und zugehörigen Ergebnisse von CodeGuru Security nach einer bestimmten Kategorie	Schreiben			
GetAccountConfiguration	Gewährt die Berechtigung zum Abrufen der Konfigurationen auf Kontoebene	Lesen			
GetFindings	Gewährt die Berechtigung zum Abrufen von Ergebnissen für einen Scan, der von CodeGuru Security generiert wurde	Auflisten	ScanName		
GetMetricsSummary	Gewährt die Berechtigung zum Abrufen der AWS Metrikzusammenfassung auf Kontoebene, die von CodeGuru Security generiert wurde	Lesen			
GetScan	Gewährt die Berechtigung zum Abrufen von Scan-Metadaten von CodeGuru Security	Lesen	ScanName		
				aws:ResourceTag/${TagKey}	
ListFindings [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Ergebnissen, die von CodeGuru Security generiert wurden	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListFindingsMetrics	Gewährt die Berechtigung zum Abrufen einer Liste von Metriken von Erkenntnissen auf Kontoebene innerhalb eines bestimmten Zeitraums	Auflisten			
ListScans	Gewährt die Berechtigung zum Abrufen der Liste der Scan-Metadaten von CodeGuru Security	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Abrufen einer Liste von Tags für einen Scannamen-ARN	Lesen	ScanName*		
				aws:ResourceTag/${TagKey}	
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einem Scannamen-ARN	Markierung	ScanName*		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags von einem Scannamen-ARN	Markierung	ScanName*		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateAccountConfiguration	Gewährt die Berechtigung zum Aktualisieren der Konfigurationen auf Kontoebene	Schreiben			

Von Amazon CodeGuru Security definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
ScanName	`arn:${Partition}:codeguru-security:${Region}:${Account}:scans/${ScanName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon CodeGuru Security

Amazon CodeGuru Security definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS CodePipeline

AWS CodePipeline (Dienstpräfix:`codepipeline`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS CodePipeline definierte Aktionen
- Von AWS CodePipeline definierte Ressourcentypen
- Bedingungsschlüssel für AWS CodePipeline

Von AWS CodePipeline definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen.

Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcknowledgeJob	Gewährt die Berechtigung zum Anzeigen von Informationen zu einem bestimmten Auftrag und ob dieser Auftrag von dem Worker empfangen wurde	Write			
AcknowledgeThirdPartyJob	Gewährt die Berechtigung, zu bestätigen, dass ein Worker den angegebenen Auftrag erhalten hat (nur Partneraktionen)	Schreiben			
CreateCustomActionType	Erteilt die Berechtigung zum Erstellen einer benutzerdefinierten Aktion, die Sie in den zugehörigen Pipelines verwenden können AWS-Konto	Schreiben	actiontype*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePipeline	Gewährt die Berechtigung zum Erstellen einer eindeutig benannten Pipeline	Schreiben	pipeline*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteCustomActionType	Gewährt die Berechtigung zum Löschen einer benutzerdefinierten Aktion	Write	actiontype*		
DeletePipeline	Gewährt die Berechtigung zum Löschen einer angegebenen Pipeline	Write	pipeline*		
DeleteWebhook	Gewährt die Berechtigung zum Löschen eines angegebenen Webhooks	Write	webhook*		
DeregisterWebhookWithThirdParty	Gewährt die Berechtigung, die Registrierung eines Webhooks bei dem in der Konfiguration angegebenen Drittanbieter zu entfernen	Write	webhook*		
DisableStageTransition	Gewährt die Berechtigung, zu verhindern, dass Revisionen zum nächsten Schritt in einer Pipeline überzugehen	Write	stage*		
EnableStageTransition	Gewährt die Berechtigung, zu gewähren, dass Revisionen zum nächsten Schritt in einer Pipeline übergehen	Schreiben	stage*		
GetActionType	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Aktion.	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetJobDetails	Gewährt die Berechtigung zum Anzeigen von Informationen zu einem Auftrag (nur benutzerdefinierte Aktionen)	Read			
GetPipeline	Gewährt die Berechtigung zum Abrufen von Informationen zur Struktur einer Pipeline	Read	pipeline*		
GetPipelineExecution	Gewährt die Berechtigung zum Anzeigen von Informationen zur Ausführung einer Pipeline, einschließlich Details zu Artefakten, Pipeline-Ausführungs-ID sowie Name, Version und Status der Pipeline	Read	pipeline*		
GetPipelineState	Gewährt die Berechtigung zum Anzeigen von Informationen über den aktuellen Status der Phasen und Aktionen einer Pipeline	Read	pipeline*		
GetThirdPartyJobDetails	Gewährt die Berechtigung zum Anzeigen der Details eines Auftrags für eine Drittanbieteraktion (nur Partneraktionen)	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListActionExecutions	Gewährt die Berechtigung zum Auflisten der Aktionsausführungen, die in einer Pipeline aufgetreten sind	Read	pipeline*		
ListActionTypes	Gewährt die Berechtigung, eine Zusammenfassung aller Aktionstypen aufzulisten, die für Pipelines in Ihrem Konto verfügbar sind	Read			
ListPipelineExecutions	Gewährt die Berechtigung zum Auflisten einer Zusammenfassung der letzten Ausführungen für eine Pipeline	Auflisten	pipeline*		
ListPipelines	Erteilt die Berechtigung, eine Zusammenfassung aller Pipelines aufzulisten, die mit Ihrem AWS-Konto	Auflisten			
ListTagsForResource	Erteilt die Berechtigung, Tags für eine CodePipeline Ressource aufzulisten	Lesen	actiontype		
			pipeline		
			webhook		
ListWebhooks	Erteilt die Erlaubnis, alle Webhooks aufzulisten, die mit Ihrem verknüpft sind AWS-Konto	Auflisten	webhook*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PollForJobs	Erteilt die Erlaubnis, Informationen über Jobs einzusehen, CodePipeline auf die Sie reagieren können	Schreiben	actiontype*		
PollForThirdPartyJobs	Gewährt die Berechtigung, zu bestimmen, ob für einen Worker auszuführende Aufträge von Drittanbietern vorhanden ist (nur Partneraktionen)	Write			
PutActionRevision	Gewährt die Berechtigung zum Bearbeiten von Aktionen in einer Pipeline	Schreiben	action*		
PutApprovalResult	Erteilt die Berechtigung, eine Antwort (Genehmigt oder Abgelehnt) auf eine manuelle Genehmigungsanfrage in zu geben CodePipeline	Schreiben	action*		
PutJobFailureResult	Gewährt die Berechtigung zur Darstellung des Fehlschlagens eines Auftrags, wie dies von einem Worker an die Pipeline zurückgegeben wurde (nur benutzerdefinierte Aktionen)	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutJobSuccessResult	Gewährt die Berechtigung zur Darstellung des Erfolgs eines Auftrags, wie dies von einem Worker an die Pipeline zurückgegeben wurde (nur benutzerdefinierte Aktionen)	Write			
PutThirdPartyJobFailureResult	Gewährt die Berechtigung zur Darstellung des Fehlschlagens eines Drittanbieterauftrags, wie dies von einem Worker an die Pipeline zurückgegeben wurde (nur Partneraktionen)	Write			
PutThirdPartyJobSuccessResult	Gewährt die Berechtigung zur Darstellung des Erfolgs eines Drittanbieterauftrags, wie dies von einem Worker an die Pipeline zurückgegeben wurde (nur Partneraktionen)	Write			
PutWebhook	Gewährt die Berechtigung zum Erstellen oder Aktualisieren eines Webhooks	Schreiben	pipeline*		
			webhook*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RegisterWebhookWithThirdParty	Gewährt die Berechtigung, einen Webhook bei dem in seiner Konfiguration angegebenen Drittanbieter zu registrieren	Write	webhook*		
RetryStageExecution	Gewährt die Berechtigung, die Pipeline-Ausführung fortzusetzen, indem die letzten fehlgeschlagenen Aktionen in einer Phase erneut versucht werden	Schreiben	stage*		
RollbackStage	Erteilt die Berechtigung, die Phase auf eine vorherige erfolgreiche Ausführung zurückzusetzen	Schreiben	stage*		
StartPipelineExecution	Gewährt die Berechtigung zum Ausführen der letzten Revision über die Pipeline	Write	pipeline*		
StopPipelineExecution	Gewährt die Berechtigung zum Beenden einer laufenden Pipeline-Ausführung	Schreiben	pipeline*		
TagResource	Erteilt die Berechtigung, eine Ressource zu taggen CodePipeline	Tagging	actiontype		
			pipeline		
			webhook		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Erteilt die Erlaubnis, ein Tag aus einer CodePipeline Ressource zu entfernen	Tagging	actiontype		
			pipeline		
			webhook		
				aws:TagKeys	
UpdateActionType	Gewährt die Berechtigung zum Aktualisieren einer Aktion.	Schreiben	actiontype*		
UpdatePipeline	Gewährt die Berechtigung zum Aktualisieren einer Pipeline mit Änderungen an der Struktur der Pipeline	Schreiben	pipeline*		

Von AWS CodePipeline definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
action	`arn:${Partition}:codepipeline:${Region}:${Account}:${PipelineName}/${StageName}/${ActionName}`	aws:ResourceTag/${TagKey}
actiontype	`arn:${Partition}:codepipeline:${Region}:${Account}:actiontype:${Owner}/${Category}/${Provider}/${Version}`	aws:ResourceTag/${TagKey}
pipeline	`arn:${Partition}:codepipeline:${Region}:${Account}:${PipelineName}`	aws:ResourceTag/${TagKey}
stage	`arn:${Partition}:codepipeline:${Region}:${Account}:${PipelineName}/${StageName}`	aws:ResourceTag/${TagKey}
webhook	`arn:${Partition}:codepipeline:${Region}:${Account}:webhook:${WebhookName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS CodePipeline

AWS CodePipeline definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung.	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf den Tag-Schlüssel-Wert-Paaren, die an die Ressource angefügt wurden.	Zeichenfolge
aws:TagKeys	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Zustandsschlüssel für AWS CodeStar

AWS CodeStar (Service-Präfix: `codestar`) bietet die folgenden service-spezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Durch AWS CodeStar definierte Aktionen
- Von AWS CodeStar definierte Ressourcentypen
- Bedingungsschlüssel für AWS CodeStar

Durch AWS CodeStar definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den

Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateTeamMember	Ermöglicht das Hinzufügen eines Benutzers zum Team für ein AWS-CodeStar-Projekt	Berechtigungsverwaltung	project*		
CreateProject	Erteilung der Berechtigung zur Erstellung eines Projekts mit minimaler Struktur, Kundenrichtlinien und ohne Ressourcen	Berechtigungsverwaltung		aws:RequestTag/${TagKey} aws:TagKeys	
CreateUserProfile	Erteilung der Berechtigung, ein Profil für einen Benutzer zu erstellen, das Benutzereinstellungen, Anzeigename und E-Mail enthält	Schreiben	user*		
DeleteExtendedAccess [nur Berechtigung]	Erteilung der Berechtigung für erweiterte Lösch-APIs	Schreiben	project*		
DeleteProject	Ermöglicht das Löschen eines Projekts, einschließlich der Projektressourcen. Löscht nicht die mit dem Projekt verbundenen Benutzer, sondern die IAM-Rollen, die den Zugriff auf das Projekt ermöglicht haben.	Berechtigungsverwaltung	project*		
DeleteUserProfile	Ermöglicht das Löschen eines Benutzerprofils in AWS	Schreiben	user*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	CodeStar, einschließlich aller mit diesem Profil verbundenen persönlichen Einstellungsdaten, wie Anzeigename und E-Mail-Adresse. Die Verlaufsdaten dieses Benutzers, z. B. die von ihm vorgenommenen Übertragungen, werden dabei nicht gelöscht.				
DescribeProject	Erteilung der Berechtigung zur Beschreibung eines Projekts und seiner Ressourcen	Lesen	project*		
DescribeUserProfile	Erteilung der Berechtigung, einen Benutzer in AWS CodeStar und die Benutzerattribute projektübergreifend zu beschreiben	Lesen			
DisassociateTeamMember	Erteilung der Berechtigung zum Entfernen eines Benutzers aus einem Projekt. Das Entfernen eines Benutzers aus einem Projekt entfernt auch die IAM-Richtlinien dieses Benutzers, die den Zugriff auf das Projekt und seine Ressourcen erlaubten	Berechtigungsverwaltung	project*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetExtendedAccess [nur Berechtigung]	Erteilung der Berechtigung für erweiterte Lese-APIs	Lesen	project*		
ListProjects	Ermöglicht die Auflistung aller Projekte in CodeStar, die Ihrem AWS-Konto zugeordnet sind	Auflisten			
ListResources	Ermöglicht die Auflistung aller mit einem Projekt verbundenen Ressourcen in CodeStar	Auflisten	project*		
ListTagsForProject	Erteilung der Berechtigung, alle mit einem Projekt verbundenen Teammitglieder aufzulisten	Auflisten	project*		
ListTeamMembers	Erteilung der Berechtigung, alle mit einem Projekt verbundenen Teammitglieder aufzulisten	Auflisten	project*		
ListUserProfiles	Erteilung der Berechtigung, Benutzerprofile in AWS CodeStar aufzulisten	Auflisten			
PutExtendedAccess [nur Berechtigung]	Erteilung der Berechtigung für erweiterte Schreib-APIs	Schreiben	project*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagProject	Ermöglicht das Hinzufügen von Tags zu einem Projekt in CodeStar	Markierung	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagProject	Ermöglicht das Entfernen von Tags aus einem Projekt in CodeStar	Markierung	project*		
				aws:TagKeys	
UpdateProject	Erteilung der Berechtigung zur Aktualisierung eines Projekts in CodeStar	Schreiben	project*		
UpdateTeamMember	Erteilung der Berechtigung zur Aktualisierung der Attribute von Teammitgliedern innerhalb eines CodeStar-Projekts	Berechtigungsverwaltung	project*		
UpdateUserProfile	Erteilung der Berechtigung zur Aktualisierung eines Benutzerprofils, das Benutzereinstellungen, Anzeigename und E-Mail enthält	Schreiben	user*		
VerifyServiceRole	Erteilung der Berechtigung zur Überprüfung, ob die AWS-CodeStar-Servicerolle im Kundenkonto vorhanden ist	Auflisten			

Von AWS CodeStar definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
project	`arn:${Partition}:codestar:${Region}:${Account}:project/${ProjectId}`	aws:ResourceTag/${TagKey}
user	`arn:${Partition}:iam::${Account}:user/${AwsUserName}`	iam:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS CodeStar

AWS CodeStar definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filterung des Zugriffs durch Anfragen auf der Grundlage der zulässigen Werte für jedes der Tags	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Zugriff nach Aktionen, basierend auf dem Tag-Wert, der der Ressource zugeordnet ist	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert den Zugriff auf Anfragen nach dem Vorhandensein von obligatorischen Tags in der Anfrage	ArrayOfString
iam:ResourceTag/${TagKey}	Filtert Zugriff nach Aktionen, basierend auf dem Tag-Wert, der der Ressource zugeordnet ist	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für AWS CodeStar Connections

AWS CodeStar Connections (Servicepräfix: `codestar-connections`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS CodeStar Connections definierte Aktionen
- Von AWS CodeStar Connections definierte Ressourcentypen
- Bedingungsschlüssel für AWS CodeStar Connections

Von AWS CodeStar Connections definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateConnection	Gewährt die Berechtigung zum Erstellen einer Verbindungsressource.	Write		aws:RequestTag/${TagKey} aws:TagKeys codestar-connections:ProviderType	
CreateHost	Gewährt die Berechtigung zum Erstellen einer Host-Ressource	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys codestar-connections:ProviderType	
CreateRepositoryLink	Gewährt die Berechtigung zum Erstellen eines Repository-Links	Schreiben	Connection*		codestar-connections:PassConnection codestar-connections:UseConnection

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSyncConfiguration	Gewährt die Berechtigung zum Erstellen einer Vorlage für die Sync-Konfiguration	Schreiben	RepositoryLink*		codestar-connections:PassRepository iam:PassRole
				codestar-connections:Branch	
DeleteConnection	Gewährt die Berechtigung zum Löschen einer Verbindungsressource.	Write	Connection*		
DeleteHost	Gewährt die Berechtigung zum Löschen einer Host-Ressource	Schreiben	Host*		
DeleteRepositoryLink	Gewährt die Berechtigung zum Löschen eines Repository-Links	Schreiben	RepositoryLink*		
DeleteSyncConfiguration	Gewährt die Berechtigung zum Löschen einer Synchronisierungskonfiguration	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetConnection	Gewährt die Berechtigung zum Abrufen von Details zu einer Verbindungsressource.	Read	Connection*		
GetHost	Gewährt die Berechtigung zum Abrufen von Details über eine Host-Ressource	Read	Host*		
GetIndividualAccessToken [nur Berechtigung]	Gewährt die Berechtigung, einen Drittanbieter, z. B. eine Bitbucket-App-Installation, mit einer Verbindung zu verknüpfen	Read		codestar-connections:ProviderType	codestar-connections:StartOAuthHandshake
GetInstallationUrl [nur Berechtigung]	Gewährt die Berechtigung, einen Drittanbieter, z. B. eine Bitbucket-App-Installation, mit einer Verbindung zu verknüpfen	Lesen		codestar-connections:ProviderType	
GetRepositoryLink	Gewährt die Berechtigung zum Beschreiben eines Repository-Links	Lesen	RepositoryLink*		
GetRepositorySyncStatus	Gewährt die Berechtigung zum Abrufen des neuesten Synchronisierungsstatus für ein Repository	Lesen	RepositoryLink*		
				codestar-connections:Branch	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetResourceSyncStatus	Gewährt die Berechtigung zum Abrufen des neuesten Synchronisierungsstatus für eine Ressource (CFN-Stack oder andere Ressourcen)	Lesen			
GetSyncBlockerSummary	Gewährt die Berechtigung zum Beschreiben von Service-Synchronisierungssperren für eine Ressource (CFN-Stack oder andere Ressourcen)	Lesen			
GetSyncConfiguration	Gewährt die Berechtigung, eine Synchronisierungskonfiguration zu beschreiben	Lesen			
ListConnections	Gewährt die Berechtigung zum Auflisten von Verbindungsressourcen.	List	Connection*		
				codestar-connections:ProviderTypeFilter	
ListHosts	Gewährt die Berechtigung zum Auflisten von Host-Ressourcen	List		codestar-connections:ProviderTypeFilter	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListInstallationTargets [nur Berechtigung]	Gewährt die Berechtigung, einen Drittanbieter, z. B. eine Bitbucket-App-Installation, mit einer Verbindung zu verknüpfen	Auflisten			codestar-connections:GetIndividualAccessToken codestar-connections:StartOAuthHandshake
ListRepositoryLinks	Gewährt die Berechtigung zum Auflisten von Repository-Links	Auflisten			
ListRepositorySyncDefinitions	Gewährt die Berechtigung zum Auflisten von Sync-Definitionen	Auflisten			
ListSyncConfigurations	Gewährt die Berechtigung zum Auflisten der Synchronisierungskonfigurationen für einen Repository-Link	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Abrufen von Schlüssel-Wert-Paaren, die verwendet werden, um die Ressource zu verwalten.	Auflisten	Connection		
			Host		
			RepositoryLink		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PassConnection [nur Berechtigung]	Gewährt die Berechtigung zum Übergeben einer Verbindungsressource an einen AWS-Service, der ein Verbindungs-ARN als Eingabe akzeptiert, z. B. codepipeline:CreatePipeline.	Read	Connection*		
				codestar-connections:PassedToService	
PassRepository [nur Berechtigung]	Gewährt die Berechtigung zum Übergeben eines Repository-Links an einen AWS-Service, der eine RepositoryLinkId als Eingabe akzeptiert, z. B. codestar-connections:CreateSyncConfiguration.	Lesen	RepositoryLink*		
				codestar-connections:PassedToService	
RegisterAppCode [nur Berechtigung]	Gewährt die Berechtigung, einen Server eines Drittanbieters, z. B. eine GitHub Enterprise Server-Instance, mit einem Host zu verknüpfen	Read		codestar-connections:HostArn	
StartAppRegistrationHandshake [nur Berechtigung]	Gewährt die Berechtigung, einen Server eines Drittanbieters, z. B. eine GitHub Enterprise Server-Instance, mit einem Host zu verknüpfen	Read		codestar-connections:HostArn	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartOAuthHandshake [nur Berechtigung]	Gewährt die Berechtigung, einen Drittanbieter, z. B. eine Bitbucket-App-Installation, mit einer Verbindung zu verknüpfen	Lesen		codestar-connections:ProviderType	
TagResource	Gewährt die Berechtigung zum Hinzufügen oder Ändern der Tags zur angegebenen Ressource	Markierung	Connection		
			Host		
			RepositoryLink		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer AWS-Ressource	Markierung	Connection		
			Host		
			RepositoryLink		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateConnectionInstallation	Gewährt die Berechtigung zum Aktualisieren einer Verbindungsressource durch eine Installation der CodeStar Connections App.	Write	Connection*		codestar-connections:GetIndividualAccessToken codestar-connections:GetInstallationUrl codestar-connections:ListInstallationTargets codestar-connections:StartOAuthHandshake
				codestar-connections:InstallationId	
UpdateHost	Gewährt die Berechtigung zum Aktualisieren einer Hostressource	Schreiben	Host*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateRepositoryLink	Gewährt die Berechtigung zum Aktualisieren eines Repository-Links	Schreiben	RepositoryLink*		
UpdateSyncBlocker	Gewährt die Berechtigung, einen Synchronisierungs-Blocker für eine Ressource (CFN-Stack oder andere Ressourcen) zu aktualisieren	Schreiben			
UpdateSyncConfiguration	Gewährt die Berechtigung zum Aktualisieren einer Synchronisierungskonfiguration.	Schreiben		codestar-connections:Branch	
UseConnection [nur Berechtigung]	Gewährt die Berechtigung, eine Verbindungsressource zum Aufrufen von Anbieteraktionen zu verwenden	Read	Connection*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				codestar-connections:BranchName codestar-connections:FullRepositoryId codestar-connections:OwnerId codestar-connections:ProviderAction codestar-connections:ProviderPermissionsRequired codestar-connections:RepositoryName	

Von AWS CodeStar Connections definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Connection	`arn:${Partition}:codestar-connections:${Region}:${Account}:connection/${ConnectionId}`	aws:ResourceTag/${TagKey}
Host	`arn:${Partition}:codestar-connections:${Region}:${Account}:host/${HostId}`	aws:ResourceTag/${TagKey}
RepositoryLink	`arn:${Partition}:codestar-connections:${Region}:${Account}:repository-link/${RepositoryLinkId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS CodeStar Connections

AWS CodeStar Connections definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString
codestar-connections:Branch	Filtert den Zugriff nach dem Zweignamen, der in der Anforderung übergeben wird	Zeichenfolge
codestar-connections:BranchName	Filtert den Zugriff nach dem Zweignamen, der in der Anforderung übergeben wird. Gilt nur für UseConnection-Anforderungen für den Zugriff auf einen bestimmten Repository-Zweig.	Zeichenfolge
codestar-connections:FullRepositoryId	Filtert den Zugriff durch das Repository, das in der Anforderung übergeben wird. Gilt nur für UseConnection-Anforderungen für den Zugriff auf ein bestimmtes Repository.	Zeichenfolge
codestar-connections:HostArn	Filtert den Zugriff durch die Host-Ressource, die mit der in der Anforderung verwendeten Verbindung verknüpft ist	ARN
codestar-connections:InstallationId	Filtert den Zugriff durch die Drittanbieter-ID (z. B. die Bitbucket-App-Installations-ID für CodeStar Connections), die zum Aktualisieren einer Verbindung verwendet wird. Ermöglicht Ihnen, einzuschränken, welche App-Installationen von Drittanbietern zum Herstellen einer Verbindung verwendet werden können.	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
codestar-connections:OwnerId	Filtert den Zugriff durch den Eigentümer des Drittanbieter-Repositorys. Gilt nur für UseConnection-Anforderungen für den Zugriff auf Repositorys, die einem bestimmten Benutzer gehören.	Zeichenfolge
codestar-connections:PassedToService	Filtert den Zugriff nach dem Service, an den der Prinzipal eine Verbindung oder einen Repository-Link übergeben darf.	Zeichenfolge
codestar-connections:ProviderAction	Filtert den Zugriff durch die Anbieteraktion in einer UseConnection-Anforderung wie ListRepositories. Alle gültigen Werte finden Sie in der Dokumentation.	ArrayOfString
codestar-connections:ProviderPermissionsRequired	Filtert den Zugriff nach den Schreibberechtigungen einer Anbieteraktion in einer UseConnection-Anforderung. Gültige Typen umfassen read_only und read_write.	Zeichenfolge
codestar-connections:ProviderType	Filtert den Zugriff nach dem Typ des Drittanbieters, der in der Anforderung übergeben wurde.	Zeichenfolge
codestar-connections:ProviderTypeFilter	Filtert den Zugriff nach dem Typ des Drittanbieters, der zum Filtern der Ergebnisse verwendet wird.	Zeichenfolge
codestar-connections:RepositoryName	Filtert den Zugriff nach dem Repository-Namen, der in der Anforderung übergeben wird. Gilt nur für UseConnection-Anforderungen für den Zugriff auf Repositorys, die einem bestimmten Benutzer gehören.	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für AWS CodeStar Notifications

AWS CodeStar Notifications (Servicepräfix: `codestar-notifications`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS CodeStar Notifications definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie

den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateNotificationRule	Gewährt die Berechtigung zum Erstellen einer Benachrichtigungsregel für eine Ressource	Write	notificationrule*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				codestar-notifications:NotificationsForResource	
DeleteNotificationRule	Gewährt die Berechtigung zum Löschen einer Benachrichtigungsregel für eine Ressource	Write	notificationrule*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	
DeleteTarget	Gewährt die Berechtigung zum Löschen eines Ziels für eine Benachrichtigungsregel	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeNotificationRule	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Benachrichtigungsregel	Read	notificationrule*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	
ListEventTypes	Gewährt die Berechtigung zum Auflisten von Benachrichtigungsereignistypen	List			
ListNotificationRules	Gewährt die Berechtigung zum Auflisten von Benachrichtigungsregeln in einem AWS-Konto	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags, die an den ARN einer Benachrichtigungsregelressource angefügt sind	List	notificationrule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListTargets	Gewährt die Berechtigung zum Auflisten der Benachrichtigungsregelziele für ein AWS-Konto	List		aws:RequestTag/${TagKey} aws:TagKeys	
Subscribe	Gewährt die Berechtigung zum Erstellen einer Mapping zwischen einer Benachrichtigungsregel und einem Amazon SNS-Thema	Write	notificationrule*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	
TagResource	Gewährt die Berechtigung zum Anfügen von Ressourcen-Tags an den ARN einer Benachrichtigungsregelressource	Markieren	notificationrule*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Unsubscribe	Gewährt die Berechtigung zum Entfernen einer Mapping zwischen einer Benachrichtigungsregel und einem Amazon SNS-Thema	Write	notificationrule*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	
UntagResource	Gewährt die Berechtigung zum Trennen von Ressourcen-Tags vom ARN einer Benachrichtigungsregelressource	Markieren	notificationrule*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateNotificationRule	Gewährt die Berechtigung zum Ändern einer Benachrichtigungsregel für eine Ressource	Write	notificationrule*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	

Von AWS CodeStar Notifications definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
notificationrule	`arn:${Partition}:codestar-notifications:${Region}:${Account}:notificationrule/${NotificationRuleId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS CodeStar Notifications

AWS CodeStar Notifications definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung.	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf den Tag-Schlüssel-Wert-Paaren, die an die Ressource angefügt wurden.	Zeichenfolge
aws:TagKeys	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString
codestar-notifications:NotificationsForResource	Filtert den Zugriff basierend auf dem ARN der Ressource, für die Benachrichtigungen konfiguriert sind	ARN

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon CodeWhisperer

Amazon CodeWhisperer (Servicepräfix: `codewhisperer`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon CodeWhisperer definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AllowVendedLogDeliveryForResource [nur Berechtigung]	Gewährt die Berechtigung zum Konfigurieren der Übermittlung von versendeten Protokollen für die CodeWhisperer-Anpassungsressource	Berechtigungsverwaltung	customization*		
				aws:ResourceTag/${TagKey}	
AssociateCustomizationPermission [nur Berechtigung]	Gewährt die Berechtigung zum Aufrufen von Associate CustomizationPermission auf CodeWhisperer	Schreiben	customization*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCustomization [nur Berechtigung]	Gewährt die Berechtigung zum Aufrufen von CreateCustomization auf CodeWhisperer	Schreiben	customization*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateProfile [nur Berechtigung]	Gewährt die Berechtigung zum Aufrufen von CreateProfile auf CodeWhisperer	Schreiben	profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteCustomization [nur Berechtigung]	Gewährt die Berechtigung zum Aufrufen von DeleteCustomization auf CodeWhisperer	Schreiben	customization*		
				aws:ResourceTag/${TagKey}	
DeleteProfile [nur Berechtigung]	Gewährt die Berechtigung zum Aufrufen von DeleteProfile auf CodeWhisperer	Schreiben	profile*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateCustomizationPermission [nur Berechtigung]	Gewährt die Berechtigung zum Aufrufen von DisassociateCustomizationPermission auf CodeWhisperer	Schreiben	customization*		
				aws:ResourceTag/${TagKey}	
GenerateRecommendations [nur Berechtigung]	Gewährt die Berechtigung zum Aufrufen von GenerateRecommendations auf CodeWhisperer	Lesen			
GetCustomization [nur Berechtigung]	Gewährt die Berechtigung zum Aufrufen von GetCustomization auf CodeWhisperer	Lesen	customization*		
				aws:ResourceTag/${TagKey}	
ListCustomizationPermissions [nur Berechtigung]	Gewährt die Berechtigung zum Aufrufen von ListCustomizationPermissions auf CodeWhisperer	Auflisten	customization*		
				aws:ResourceTag/${TagKey}	
ListCustomizationVersions [nur Berechtigung]	Gewährt die Berechtigung zum Aufrufen von ListCustomizationVersions auf CodeWhisperer	Auflisten	customization*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListCustomizations [nur Berechtigung]	Gewährt die Berechtigung zum Aufrufen von ListCustomizations auf CodeWhisperer	Auflisten	customization*		
ListProfiles [nur Berechtigung]	Gewährt die Berechtigung zum Aufrufen von ListProfiles auf CodeWhisperer	Auflisten			
ListTagsForResource [nur Berechtigung]	Gewährt die Berechtigung zum Aufrufen von ListTagsForResource auf CodeWhisperer	Auflisten	customization		
			profile		
				aws:ResourceTag/${TagKey}	
TagResource [nur Berechtigung]	Gewährt die Berechtigung zum Aufrufen von TagResource auf CodeWhisperer	Markierung	customization		
			profile		
				aws:ResourceTag/${TagKey} aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UntagResource [nur Berechtigung]	Gewährt die Berechtigung zum Aufrufen von UntagResource auf CodeWhisperer	Markierung	customization		
			profile		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCustomization [nur Berechtigung]	Gewährt die Berechtigung zum Aufrufen von UpdateCustomization auf CodeWhisperer	Schreiben	customization*		
				aws:ResourceTag/${TagKey}	
UpdateProfile [nur Berechtigung]	Gewährt die Berechtigung zum Aufrufen von UpdateProfile auf CodeWhisperer	Schreiben	profile*		
				aws:ResourceTag/${TagKey}	

Von Amazon CodeWhisperer definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
profile	`arn:${Partition}:codewhisperer::${Account}:profile/${Identifier}`	aws:ResourceTag/${TagKey}
customization	`arn:${Partition}:codewhisperer::${Account}:customization/${Identifier}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon CodeWhisperer

Amazon CodeWhisperer definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der CodeWhisperer-Ressource zugeordnet sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Cognito Identity

Amazon Cognito Identity (Servicepräfix: `cognito-identity`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Cognito Identity definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateIdentityPool	Gewährt die Berechtigung zum Erstellen eines neuen Identitäten-Pools	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteIdentities	Gewährt die Berechtigung zum Löschen von Identitäten aus einem Identitäten-Pool. Sie können eine Liste mit 1 bis 60 Identitäten zum Löschen angeben	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteIdentityPool	Gewährt die Berechtigung zum Löschen eines Benutzerpools. Sobald ein Pool gelöscht wird, können die Benutzer keine Authentifizierung mit dem Pool mehr durchführen	Write	identitypool*		
DescribeIdentity	Gewährt die Berechtigung zur Ausgabe von Metadaten im Zusammenhang mit der angegebenen Identität einschließlich Erstellungszeitpunkt der Identität und zugeordneter verknüpfter Anmeldungen	Read			
DescribeIdentityPool	Gewährt die Berechtigung zum Abrufen von Informationen zu einem bestimmten Identitäten-Pool, einschließlich Pool-Name, ID-Beschreibung, Erstellungsdatum und aktueller Anzahl von Benutzern	Read	identitypool*		
GetCredentialsForIdentity	Gewährt die Berechtigung zur Ausgabe von Anmeldeinformationen für die bereitgestellte Identitäts-ID	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetId	Gewährt die Berechtigung zum Generieren einer Cognito-ID (oder zum Abrufen). Durch das Angeben mehrerer Anmeldungen wird ein implizit verknüpftes Konto erstellt	Schreiben			
GetIdentityPoolAnalytics	Gewährt die Berechtigung zum Abrufen von Analysedaten über die gesamte aktuelle Identitätsanzahl für alle Identitätspool-Identitätsanbieter (IdPs)	Lesen	identitypool*		
GetIdentityPoolDailyAnalytics	Gewährt die Berechtigung zum Abrufen von Analysedaten über die Anzahl neuer Identitäten und die Gesamtzahl der Identitäten für alle Identitätspool-Identitätsanbieter (IdPs)	Lesen	identitypool*		
GetIdentityPoolRoles	Gewährt die Berechtigung zum Abrufen der Rollen für einen Identitäten-Pool	Lesen	identitypool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetIdentityProviderDailyAnalytics	Gewährt die Berechtigung zum Abrufen von Analysedaten über die Anzahl neuer Identitäten und die Gesamtzahl der Identitäten für einen Identitätspool-Identitätsanbieter (IdPs)	Lesen	identitypool*		
GetOpenIdToken	Gewährt die Berechtigung zum Abrufen eines OpenID-Tokens unter Verwendung einer bekannten Cognito-ID	Read			
GetOpenIdTokenForDeveloperIdentity	Gewährt die Berechtigung zum Registrieren (oder Abrufen) einer Cognito IdentityId und eines OpenID Connect-Token für einen Benutzer, der durch Ihren Backend-Authentifizierungsprozess überprüft wird	Read	identitypool*		
GetPrincipalTagAttributeMap	Gewährt die Berechtigung zum Abrufen der Prinzipal-Tags für einen Identitäten-Pool und einen Anbieter	Read	identitypool*		
ListIdentities	Gewährt die Berechtigung zum Auflisten von Identitäten in einem Identitäten-Pool	List	identitypool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListIdentityPools	Gewährt die Berechtigung zum Auflisten aller Cognito-Identitäten-Pools, die für Ihr Konto registriert sind	List			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags, die einem Amazon Cognito-Identitäten-Pool zugeordnet sind	Read	identitypool		
LookupDeveloperIdentity	Gewährt die Berechtigung zum Abrufen der IdentityID, die einem DeveloperUserIdentifier zugeordnet ist, oder der Liste der DeveloperUserIdentifiers, die einer IdentityId für eine vorhandene Identität zugeordnet sind	Read	identitypool*		
MergeDeveloperIdentities	Gewährt die Berechtigung zum Zusammenführen von zwei Benutzern mit unterschiedlichen IdentityIds, die sich in demselben Identitäten-Pool befinden und von demselben Entwickleranbieter identifiziert werden	Write	identitypool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SetIdentityPoolRoles	Gewährt die Berechtigung zum Festlegen der Rollen für einen Identitäten-Pool. Diese Rollen werden für Aufrufe der GetCredentialsForIdentity-Aktion verwendet	Write			
SetPrincipalTagAttributeMap	Gewährt die Berechtigung zum Festlegen der Prinzipal-Tags für einen Identitäten-Pool und einen Anbieter. Diese Tags werden für Aufrufe der GetOpenIDToken-Aktion verwendet	Write			
TagResource	Gewährt die Berechtigung zum Zuweisen einer Reihe von Tags zu einem Amazon Cognito-Identitäten-Pool	Markieren	identitypool		
				aws:RequestTag/${TagKey} aws:TagKeys	
UnlinkDeveloperIdentity	Gewährt die Berechtigung zum Aufheben der Verknüpfung eines DeveloperUserIdentifier mit einer vorhandenen Identität	Write	identitypool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UnlinkIdentity	Gewährt die Berechtigung zum Aufheben der Verknüpfung eines Identitätsverbunds mit einem vorhandenen Konto	Write			
UntagResource	Gewährt die Berechtigung zum Entfernen der angegebenen Tags aus einem Amazon Cognito-Identitäten-Pool	Markieren	identitypool		
				aws:TagKeys	
UpdateIdentityPool	Gewährt die Berechtigung zum Aktualisieren eines Identitäten-Pools	Write	identitypool*		

Von Amazon Cognito Identity definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
identitypool	`arn:${Partition}:cognito-identity:${Region}:${Account}:identitypool/${IdentityPoolId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Cognito Identity

Amazon Cognito Identity definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung.	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf den Tag-Schlüssel-Wert-Paaren, die an die Ressource angefügt wurden.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch einen Schlüssel in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Cognito Sync

Amazon Cognito Sync (Servicepräfix: `cognito-sync`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Cognito Sync definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BulkPublish	Gewährt die Berechtigung für eine Massen-Veröffentlichung aller existierenden Datasets eines Identitäten-Pools im konfigurierten Stream	Schreiben	identitypool*		
DeleteDataset	Gewährt die Berechtigung zum Löschen eines bestimmten Datensatzes	Schreiben	dataset*		
DescribeDataset	Gewährt die Berechtigung zum Abrufen von Metadaten zu einem Datensatz über Identität und Datensatzname	Lesen	dataset*		
DescribeIdentityPoolUsage	Gewährt die Berechtigung zum Abrufen von Nutzungsdetails (z. B. Datenspeicher) zu einem bestimmten Identitäten-Pool	Lesen	identitypool*		
DescribeIdentityUsage	Gewährt die Berechtigung zum Abrufen von Nutzungsinformationen für eine Identität, einschließlich der Anzahl der Datensätze und der Datennutzung	Lesen	identity*		
GetBulkPublishDetails	Gewährt die Berechtigung zum Abrufen der letzten	Lesen	identitypool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	BulkPublish-Produktion für einen Identitäten-Pool				
GetCognitoEvents	Gewährt die Berechtigung zur Zuordnung der Ereignisse und der zugehörigen Lambda-Funktionen zu einem Identitäten-Pool	Lesen	identitypool*		
GetIdentityPoolConfiguration	Gewährt die Berechtigung zum Abrufen der Konfigurationseinstellungen eines Identitäten-Pools	Lesen	identitypool*		
ListDatasets	Gewährt die Berechtigung zum Auflisten von Datensätzen für eine Identität	Auflisten	dataset*		
ListIdentityPoolUsage	Gewährt die Berechtigung zum Auflisten aller Identitäten-Pools, die für Cognito registriert sind	Lesen	identitypool*		
ListRecords	Gewährt die Berechtigung zum Abrufen paginierter Datensätze, die optional nach einer bestimmten Synchronisierungszahl für einen Datensatz und eine Identität geändert wurden	Lesen	dataset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
QueryRecords [nur Berechtigung]	Gewährt die Berechtigung zum Abfragen von Datensätzen	Lesen			
RegisterDevice	Gewährt die Berechtigung zum Registrieren eines Geräts für den Empfang von Push-Synchronisierungsbenachrichtigungen	Schreiben	identity*		
SetCognitoEvents	Legt die AWS-Lambda-Funktion für einen gegebenen Ereignistyp für einen Identitäten-Pool fest	Schreiben	identitypool*		
SetDatasetConfiguration [nur Berechtigung]	Gewährt die Berechtigung zum Konfigurieren von Datensätzen	Schreiben	dataset*		
SetIdentityPoolConfiguration	Gewährt die Berechtigung zum Festlegen der erforderlichen Konfiguration für die Push-Synchronisierung	Schreiben	identitypool*		
SubscribeToDataset	Gewährt die Berechtigung für das Abonnieren von Benachrichtigungen, wenn ein Datensatz von einem anderen Gerät geändert wird	Schreiben	dataset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UnsubscribeFromDataset	Gewährt die Berechtigung zum Beenden des Abonnements zum Empfang von Benachrichtigungen, wenn ein Datensatz von einem anderen Gerät geändert wird	Schreiben	dataset*		
UpdateRecords	Gewährt die Berechtigung zum Posten von Aktualisierungen in Datensätzen sowie zum Hinzufügen und Löschen von Daten für einen Datensatz oder Benutzer	Schreiben	dataset*		

Von Amazon Cognito Sync definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
dataset	`arn:${Partition}:cognito-sync:${Region}:${Account}:identitypool/${IdentityPoolId}/identity/${IdentityId}/dataset/${DatasetName}`	

Ressource ntypen	ARN	Bedingungsschlüssel
identity	`arn:${Partition}:cognito-sync:${Region}:${Account}:identitypool/${IdentityPoolId}/identity/${IdentityId}`	
identitypool	`arn:${Partition}:cognito-sync:${Region}:${Account}:identitypool/${IdentityPoolId}`	

Bedingungsschlüssel für Amazon Cognito Sync

Cognito Sync besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Cognito-Benutzerpools

Amazon Cognito-Benutzerpools (Servicepräfix: `cognito-idp`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Cognito-Benutzerpools definierte Aktionen
- Von Amazon Cognito User Pools definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Cognito-Benutzerpools

Von Amazon Cognito-Benutzerpools definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddCustomAttributes	Gewährt die Berechtigung zum Hinzufügen von Benutzerattributen zum Benutzerpool-Schema	Schreiben	userpool*		
AdminAddUserToGroup	Gewährt die Berechtigung zum Hinzufügen jedes Benutzers zu jeder Gruppe	Schreiben	userpool*		
AdminConfirmSignUp	Gewährt die Berechtigung, die Registrierung eines Benutzers ohne Bestätigungscode zu bestätigen	Schreiben	userpool*		
AdminCreateUser	Gewährt die Berechtigung, neue Benutzer zu erstellen und Willkommensnachrichten per E-Mail oder SMS zu senden	Schreiben	userpool*		
AdminDeleteUser	Gewährt die Berechtigung zum Löschen eines beliebigen Benutzers	Schreiben	userpool*		
AdminDeleteUserAttributes	Gewährt die Berechtigung zum Löschen von Attributen eines beliebigen Benutzers	Schreiben	userpool*		
AdminDisableProviderForUser	Gewährt die Berechtigung zur Aufhebung der Verknüpfung eines beliebigen Benutzerpool-Benutzers mit einem	Schreiben	userpool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Benutzer eines dritten Identitätsanbieters (IdP)				
AdminDisableUser	Gewährt die Berechtigung zum Deaktivieren eines Benutzers	Schreiben	userpool*		
AdminEnableUser	Gewährt die Berechtigung zum Aktivieren eines Benutzers	Schreiben	userpool*		
AdminForgetDevice	Gewährt die Berechtigung zum Aufheben der Registrierung der Geräte eines Benutzers	Schreiben	userpool*		
AdminGetDevice	Gewährt die Berechtigung zum Abrufen von Informationen über die Geräte eines Benutzers	Lesen	userpool*		
AdminGetUser	Gewährt die Berechtigung, jeden Benutzer anhand des Benutzernamens nachzuschlagen	Lesen	userpool*		
AdminInitiateAuth	Gewährt die Berechtigung zum Authentifizieren eines Benutzers	Schreiben	userpool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AdminLinkProviderForUser	Gewährt die Berechtigung zum Verknüpfen eines beliebigen Benutzerpool-Benutzers mit einem Drittanbieter-IdP-Benutzer	Schreiben	userpool*		
AdminListDevices	Gewährt die Berechtigung zum Auflisten der gespeicherten Geräte eines beliebigen Benutzers	Auflisten	userpool*		
AdminListGroupsForUser	Gewährt die Berechtigung zum Auflisten der Gruppen, denen ein Benutzer angehört	Auflisten	userpool*		
AdminListUserAuthEvents	Gewährt die Berechtigung zum Auflisten von Anmeldeereignissen für beliebige Benutzer	Lesen	userpool*		
AdminRemoveUserFromGroup	Gewährt die Berechtigung zum Entfernen eines Benutzers aus einer Gruppe	Schreiben	userpool*		
AdminResetUserPassword	Gewährt die Berechtigung zum Zurücksetzen des Passworts eines beliebigen Benutzers	Schreiben	userpool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AdminRespondToAuthChallenge	Gewährt die Berechtigung, auf eine Authentifizierungsherausforderung während der Authentifizierung eines Benutzers zu reagieren	Schreiben	userpool*		
AdminSetUserMFAPreference	Gewährt die Berechtigung zum Festlegen der bevorzugten MFA-Methode eines beliebigen Benutzers	Schreiben	userpool*		
AdminSetUserPassword	Gewährt die Berechtigung zum Festlegen des Kennworts eines beliebigen Benutzers	Schreiben	userpool*		
AdminSetUserSettings	Gewährt die Berechtigung zum Festlegen von Benutzereinstellungen für beliebige Benutzer	Schreiben	userpool*		
AdminUpdateAuthEventFeedback	Gewährt die Berechtigung zum Aktualisieren des erweiterten Sicherheitsfeedbacks für das Authentifizierungsereignis eines beliebigen Benutzers	Schreiben	userpool*		
AdminUpdateDeviceStatus	Gewährt die Berechtigung zum Aktualisieren des Status der gespeicherten Geräte eines beliebigen Benutzers	Schreiben	userpool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AdminUpdateUserAttributes	Gewährt die Berechtigung zum Aktualisieren der Standard- oder benutzerdefinierten Attribute eines beliebigen Benutzers	Schreiben	userpool*		
AdminUserGlobalSignOut	Gewährt die Berechtigung zum Abmelden eines Benutzers von allen Sitzungen	Schreiben	userpool*		
AssociateSoftwareToken	Gewährt die Berechtigung, einen eindeutig generierten, gemeinsam genutzten geheimen Schlüsselcode für den Benutzer zurückzugeben	Schreiben			
AssociateWebACL [nur Berechtigung]	Gewährt die Berechtigung zum Zuordnen des Benutzerpools mit einemAWS-WAF-Web-ACL	Schreiben	userpool* webacl*		
ChangePassword	Gewährt die Berechtigung zum Ändern des Kennworts für einen angegebenen Benutzer in einem Benutzerpool	Schreiben			
ConfirmDevice	Gewährt die Berechtigung zur Bestätigung der Verfolgung des Geräts. Dieser API-Aufruf ist der Aufruf, der die Geräteverfolgung startet.	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ConfirmForgotPassword	Gewährt die Berechtigung, einem Benutzer die Eingabe eines Bestätigungscodes zum Zurücksetzen eines vergessenen Passworts zu ermöglichen	Schreiben			
ConfirmSignUp	Gewährt die Berechtigung zur Bestätigung der Registrierung eines Benutzers und verwaltet den vorhandenen Alias eines vorherigen Benutzers	Schreiben			
CreateGroup	Gewährt die Berechtigung zum Erstellen neuer Benutzerpool-Gruppen	Schreiben	userpool*		
CreateIdentityProvider	Gewährt die Berechtigung zum Hinzufügen von Identitätsanbietern zu Benutzerpools	Schreiben	userpool*		
CreateResourceServer	Gewährt die Berechtigung zum Erstellen und Konfigurieren von Bereichen für OAuth 2.0-Ressourcenserver	Schreiben	userpool*		
CreateUserImportJob	Gewährt die Berechtigung zum Erstellen von Benutzer-CSV-Importaufgaben	Schreiben	userpool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateUserPool	Gewährt die Berechtigung zum Erstellen und Festlegen von Passwortrichtlinien für Benutzerpools	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateUserPoolClient	Gewährt die Berechtigung zum Erstellen von Benutzerpool-App-Clients	Schreiben	userpool*		
CreateUserPoolDomain	Gewährt die Berechtigung zum Hinzufügen von Benutzerpool-Domains	Schreiben	userpool*		
DeleteGroup	Gewährt die Berechtigung zum Löschen einer leeren Benutzerpoolgruppe	Schreiben	userpool*		
DeleteIdentityProvider	Gewährt die Berechtigung zum Löschen beliebiger Identitätsanbieter aus Benutzerpools	Schreiben	userpool*		
DeleteResourceServer	Gewährt die Berechtigung zum Löschen beliebiger OAuth 2.0-Ressourcenserver aus Benutzerpools	Schreiben	userpool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteUser	Gewährt einem Benutzer die Berechtigung, sich selbst zu löschen	Schreiben			
DeleteUserAttributes	Gewährt die Berechtigung zum Löschen der Attribute für einen Benutzer	Schreiben			
DeleteUserPool	Gewährt die Berechtigung zum Löschen von Benutzerpools	Schreiben	userpool*		
DeleteUserPoolClient	Gewährt die Berechtigung zum Löschen eines beliebigen Benutzerpool-App-Clients	Schreiben	userpool*		
DeleteUserPoolDomain	Gewährt die Berechtigung zum Löschen einer beliebigen Benutzerpool-Domain	Schreiben	userpool*		
DescribeIdentityProvider	Gewährt die Berechtigung zum Beschreiben eines beliebigen Benutzerpool-Identitätsanbieters	Lesen	userpool*		
DescribeResourceServer	Gewährt die Berechtigung, zum Beschreiben jedes OAuth 2.0-Ressourcenservers	Lesen	userpool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeRiskConfiguration	Gewährt die Berechtigung zum Beschreiben der Risikokonfigurationseinstellungen von Benutzerpools und App-Clients	Lesen	userpool*		
DescribeUserImportJob	Gewährt die Berechtigung zum Beschreiben eines beliebigen Benutzerimportauftrags	Lesen	userpool*		
DescribeUserPool	Gewährt die Berechtigung zum Beschreiben eines Benutzerpools	Lesen	userpool*		
DescribeUserPoolClient	Gewährt die Berechtigung zum Beschreiben eines beliebigen Benutzerpool-App-Clients	Lesen	userpool*		
DescribeUserPoolDomain	Gewährt die Berechtigung zum Beschreiben einer Benutzerpool-Domain	Lesen			
DisassociateWebACL [nur Berechtigung]	Gewährt die Berechtigung zum Aufheben der Zuordnung des Benutzerpools zu einer AWS WAF-Web-ACL	Schreiben	userpool*		
ForgetDevice	Gewährt die Berechtigung zum Verlassen des angegebenen Geräts	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ForgotPassword	Gewährt die Berechtigung zum Senden einer Nachricht an den Endbenutzer mit einem Bestätigungscode, der zum Ändern des Passworts des Benutzers erforderlich ist	Schreiben			
GetCSVHeader	Gewährt die Berechtigung zum Generieren von Headern für eine Benutzerimport-CSV-Datei	Lesen	userpool*		
GetDevice	Gewährt die Berechtigung zum Abrufen des Geräts	Lesen			
GetGroup	Gewährt die Berechtigung zum Beschreiben einer Benutzerpoolgruppe	Lesen	userpool*		
GetIdentityProviderByIdentifier	Gewährt die Berechtigung, eine Benutzerpool-IdP-ID mit dem IdP-Namen zu korrelieren	Lesen	userpool*		
GetLogDeliveryConfiguration	Gewährt die Berechtigung zum Abrufen der detaillierten Konfiguration der Aktivität sprotokollierung für einen Benutzerpool	Lesen	userpool*		
GetSigningCertificate	Gewährt die Berechtigung zum Nachschlagen von Signaturzertifikaten für Benutzerpools	Lesen	userpool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetUICustomization	Gewährt die Berechtigung zum Abrufen von Anpassungsinformationen für die gehostete Benutzeroberfläche eines beliebigen App-Clients	Lesen	userpool*		
GetUser	Gewährt die Berechtigung zum Abrufen der Benutzerattribute und Metadaten für einen Benutzer	Lesen			
GetUserAttributeVerificationCode	Gewährt die Berechtigung zum Abrufen des Verifizierungscodes des Benutzerattributs für den angegebenen Attributnamen	Lesen			
GetUserPoolMfaConfig	Gewährt die Berechtigung zum Nachschlagen der MFA-Konfiguration eines Benutzerpools	Lesen	userpool*		
GetWebACLForResource [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen der AWS-WAF-Web-ACL, die einem Amazon Cognito-Benutzerpool zugeordnet ist	Lesen	userpool*		
GlobalSignOut	Gewährt die Berechtigung zum Abmelden von Benutzern von allen Geräten	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
InitiateAuth	Gewährt die Berechtigung zum Initiieren des Authentifizierungsablaufs	Schreiben			
ListDevices	Gewährt die Berechtigung zum Auflisten der Geräte	Auflisten			
ListGroups	Gewährt die Berechtigung zum Auflisten aller Gruppen in Benutzerpools	Auflisten	userpool*		
ListIdentityProviders	Gewährt die Berechtigung zum Auflisten aller Identitätsanbieter in Benutzerpools	Auflisten	userpool*		
ListResourceServers	Gewährt die Berechtigung zum Auflisten aller Ressourcenserver in Benutzerpools	Auflisten	userpool*		
ListResourcesForWebACL [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der Benutzerpools, die einer AWS WAF-Web-ACL zugeordnet sind	Auflisten	webacl*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags, die einem Amazon Cognito-Benutzerpool zugeordnet sind	Auflisten	userpool		
ListUserImportJobs	Gewährt die Berechtigung zum Auflisten aller Benutzerimportaufträge	Auflisten	userpool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListUserPoolClients	Gewährt die Berechtigung zum Auflisten aller App-Clients in Benutzerpools	Auflisten	userpool*		
ListUserPools	Gewährt die Berechtigung zum Auflisten aller Benutzerpools	Auflisten			
ListUsers	Gewährt die Berechtigung zum Auflisten aller Benutzerpool-Benutzer	Auflisten	userpool*		
ListUsersInGroup	Gewährt die Berechtigung zum Auflisten von Benutzern in einer beliebigen Gruppe	Auflisten	userpool*		
ResendConfirmationCode	Gewährt die Berechtigung zum erneuten Senden der Bestätigung (zur Bestätigung der Registrierung) an einen bestimmten Benutzer im Benutzerpool	Schreiben			
RespondToAuthChallenge	Gewährt die Berechtigung, auf die Authentifizierungsaufforderung zu antworten	Schreiben			
RevokeToken	Gewährt die Berechtigung zum Aufheben aller durch das angegebene Aktualisierungstoken generierten Zugriffstoken	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SetLogDeliveryConfiguration	Gewährt die Berechtigung zum Einrichten oder Ändern der Konfiguration der Aktivitätsprotokollierung eines Benutzerpools	Schreiben	userpool*		
SetRiskConfiguration	Gewährt die Berechtigung, die Risikokonfiguration für Benutzerpools und App-Clients festzulegen	Schreiben	userpool*		
SetUICustomization	Gewährt die Berechtigung zum Anpassen der gehosteten Benutzeroberfläche für einen App-Client	Schreiben	userpool*		
SetUserMFAPreference	Gewährt die Berechtigung zum Festlegen der MFA-Präferenz für den Benutzer im Benutzerpool	Schreiben			
SetUserPoolMfaConfig	Gewährt die Berechtigung zum Festlegen einer Benutzerpool-MFA-Konfiguration	Schreiben	userpool*		
SetUserSettings	Gewährt die Berechtigung zum Festlegen von Benutzereinstellungen wie der Multi-Faktor-Authentifizierung (MFA)	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SignUp	Gewährt die Berechtigung zur Registrierung des Benutzers im angegebenen Benutzerpool und erstellt einen Benutzernamen, ein Kennwort und Benutzerattribute	Schreiben			
StartUserImportJob	Gewährt die Berechtigung zum Starten eines Benutzerimportauftrags	Schreiben	userpool*		
StopUserImportJob	Gewährt die Berechtigung zum Stoppen eines Benutzerimportauftrags	Schreiben	userpool*		
TagResource	Gewährt die Berechtigung zum Markieren eines Benutzerpools	Markierung	userpool		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entmarkieren eines Benutzerpools	Markierung	userpool		
				aws:TagKeys	
UpdateAuthEventFeedback	Gewährt die Berechtigung zum Aktualisieren des Feedbacks für das Benutzer-Authentifizierungsereignis	Schreiben	userpool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateDeviceStatus	Gewährt die Berechtigung zum Aktualisieren des Gerätestatus	Schreiben			
UpdateGroup	Gewährt die Berechtigung zum Aktualisieren der Konfiguration einer Gruppe	Schreiben	userpool*		
UpdateIdentityProvider	Gewährt die Berechtigung zum Aktualisieren der Konfiguration eines beliebigen Benutzerpool-IdP	Schreiben	userpool*		
UpdateResourceServer	Gewährt die Berechtigung zum Aktualisieren der Konfiguration eines beliebigen OAuth 2.0-Ressourcenservers	Schreiben	userpool*		
UpdateUserAttributes	Gewährt einem Benutzer die Berechtigung, ein bestimmtes Attribut (jeweils eines) zu aktualisieren	Schreiben			
UpdateUserPool	Gewährt die Berechtigung zum Aktualisieren der Konfiguration eines Benutzerpools	Schreiben	userpool*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateUserPoolClient	Gewährt die Berechtigung zum Aktualisieren eines Benutzerpool-Clients	Schreiben	userpool*		
UpdateUserPoolDomain	Gewährt die Berechtigung zum Ersetzen des Zertifikats für eine benutzerdefinierte Domain	Schreiben	userpool*		
VerifySoftwareToken	Gewährt die Berechtigung, den eingegebenen TOTP-Code eines Benutzers zu registrieren und den MFA-Status des Software-Tokens des Benutzers bei Erfolg als verifiziert zu markieren	Schreiben			
VerifyUserAttribute	Gewährt die Berechtigung zur Überprüfung eines Benutzerattributs mithilfe eines einmaligen Bestätigungscodes	Schreiben			

Von Amazon Cognito User Pools definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
userpool	`arn:${Partition}:cognito-idp:${Region}:${Account}:userpool/${UserPoolId}`	aws:ResourceTag/${TagKey}
webacl	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/webacl/${Name}/${Id}`	

Bedingungsschlüssel für Amazon Cognito-Benutzerpools

Amazon Cognito-Benutzerpools definieren die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch einen Schlüssel in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Comprehend

Amazon Comprehend (Servicepräfix: `comprehend`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Comprehend definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchDetectDominantLanguage	Gewährt die Berechtigung zum Erkennen der Sprache oder der Sprachen, die in der Liste der Textdokumente enthalten sind	Read			
BatchDetectEntities	Gewährt die Berechtigung, die benannten Entitäten („Personen“, „Orte“, „Standorte“ usw.) in der angegebenen Liste von Textdokumenten zu erkennen	Read			
BatchDetectKeyPhrases	Gewährt die Berechtigung, die Ausdrücke in der Liste von	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Textdokumenten zu erkennen, die in Bezug auf den Inhalt am aussagekräftigsten sind				
BatchDetectSentiment	Gewährt die Berechtigung, die Stimmung eines Texts in der Dokumentliste zu erkennen (positiv, negativ, neutral oder gemischt)	Read			
BatchDetectSyntax	Gewährt die Berechtigung, syntaktische Informationen (wie Wortart, Token) in einer Liste von Textdokumenten zu erkennen	Lesen			
BatchDetectTargetedSentiment	Erteilt die Erlaubnis, die mit bestimmten Entitäten (z. B. Marken oder Produkten) verbundenen Stimmungen innerhalb der angegebenen Liste von Textdokumenten zu erkennen	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ClassifyDocument	Gewährt die Berechtigung zum Erstellen einer neuen Dokumentenklassifizierungsanforderung, um ein einzelnes Dokument in Echtzeit zu analysieren, wobei ein zuvor erstelltes und trainiertes benutzerdefiniertes Modell und ein Endpunkt verwendet werden	Lesen	document-classifier-endpoint*		
ContainsPiiEntities	Gewährt die Berechtigung zum Klassifizieren der personenbezogenen Daten in bestimmten Dokumenten in Echtzeit	Lesen			
CreateDataset	Gewährt die Berechtigung zum Erstellen eines neuen Datensatzes in einem Flywheel	Schreiben	flywheel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDocumentClassifier	Gewährt die Berechtigung zum Erstellen eines neuen Dokumentklassifizierers, mit dem Sie Dokumente kategorisieren können	Write	document-classifier*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateEndpoint	Gewährt die Berechtigung, einen modellspezifischen Endpunkt zur synchronen Inferenz für ein zuvor trainiertes benutzerdefiniertes Modell zu erstellen.	Write	document-classifier*		
			document-classifier-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys	
			entity-recognizer*		
			entity-recognizer-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys	
			flywheel		
CreateEntityRecognizer	Gewährt die Berechtigung zum Erstellen einer Entitätserkennung mit übermittelten Dateien	Schreiben	entity-recognizer*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateFlywheel	Gewährt die Berechtigung zum Erstellen eines neuen Flywheel, mit dem Sie Modellversionen trainieren können	Schreiben	flywheel*	aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:DataLakeKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			document-classifier		
			entity-recognizer		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteDocumentClassifier	Gewährt die Berechtigung zum Löschen eines zuvor erstellten Dokumentklassifizierers	Write	document-classifier*		
DeleteEndpoint	Gewährt die Berechtigung zum Löschen eines modellspezifischen Endpunkts für ein zuvor geschultes benutzerdefiniertes Modell. Alle Endpunkte müssen gelöscht werden, damit das Modell gelöscht werden kann.	Write	document-classifier-endpoint*		
			entity-recognizer-endpoint*		
DeleteEntityRecognizer	Gewährt die Berechtigung zum Löschen einer übermittelten Entität	Schreiben	entity-recognizer*		
DeleteFlywheel	Gewährt die Berechtigung zum Löschen eines Flywheel	Schreiben	flywheel*		
DeleteResourcePolicy	Gewährt die Berechtigung zum Entfernen einer Richtlinie aus einer Ressource	Schreiben	document-classifier*		
			entity-recognizer*		
DescribeDataset	Gewährt die Berechtigung zum Abrufen der Eigenschaften, die einem Datensatz zugeordnet sind	Lesen	flywheel-dataset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDocumentClassificationJob	Gewährt die Berechtigung zum Abrufen der Eigenschaften, die einem Dokumentklassifizierungsauftrag zugeordnet sind	Read	document-classification-job*		
DescribeDocumentClassifier	Gewährt die Berechtigung zum Abrufen der Eigenschaften, die einem Dokumentklassifizierer zugeordnet sind	Read	document-classifier*		
DescribeDominantLanguageDetectionJob	Gewährt die Berechtigung zum Abrufen der Eigenschaften, die einem dominanten Spracherkennungsauftrag zugeordnet sind	Read	dominant-language-detection-job*		
DescribeEndpoint	Gewährt die Berechtigung zum Abrufen der Eigenschaften, die einem bestimmten Endpunkt zugeordnet sind. Verwenden Sie diesen Vorgang, um den Status eines Endpunkts abzurufen.	Read	document-classifier-endpoint*		
			entity-recognizer-endpoint*		
DescribeEntitiesDetectionJob	Gewährt die Berechtigung zum Abrufen der Eigenschaften, die einem Entitätserkennungsauftrag zugeordnet sind	Read	entities-detection-job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeEntityRecognizer	Gewährt die Berechtigung zur Bereitstellung von Details über eine Entitätserkennung, einschließlich Status, S3-Buckets mit Trainingsdaten, Erkennungsmetadaten, Metriken und so weiter.	Read	entity-recognizer*		
DescribeEventsDetectionJob	Gewährt die Berechtigung, die einer Ereigniserkennungsaufgabe zugeordneten Eigenschaften abzurufen	Lesen	events-detection-job*		
DescribeFlywheel	Gewährt die Berechtigung zum Abrufen der Eigenschaften, die einem Flywheel zugeordnet sind	Lesen	flywheel*		
DescribeFlywheelIteration	Gewährt die Berechtigung zum Abrufen der Eigenschaften, die einer Flywheel-Iteration für ein Flywheel zugeordnet sind	Lesen	flywheel*		
				comprehend:FlywheelIterationId	
DescribeKeyPhrasesDetectionJob	Gewährt die Berechtigung zum Abrufen der Eigenschaften, die mit einem Schlüsselphrasen-Erkennungsauftrag zugeordnet sind	Read	key-phrases-detection-job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribePiiEntitiesDetectionJob	Gewährt die Berechtigung zum Abrufen der Eigenschaften, die einem PII-Entitätserkennungsauftrag zugeordnet sind	Lesen	pii-entities-detection-job*		
DescribeResourcePolicy	Gewährt die Berechtigung zum Lesen einer an die Ressource angefügte Richtlinie	Lesen	document-classifier*		
			entity-recognizer*		
DescribeSentimentDetectionJob	Gewährt die Berechtigung zum Abrufen der Eigenschaften, die mit einem Stimmungserkennungsauftrag zugeordnet sind	Lesen	sentiment-detection-job*		
DescribeTargetedSentimentDetectionJob	Gewährt die Berechtigung zum Abrufen der Eigenschaften, die einem Stimmungserkennungsauftrag zugeordnet sind	Lesen	targeted-sentiment-detection-job*		
DescribeTopicsDetectionJob	Gewährt die Berechtigung zum Abrufen der Eigenschaften, die einem Themenerkennungsauftrag zugeordnet sind	Read	topics-detection-job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DetectDominantLanguage	Gewährt die Berechtigung zum Erkennen der im Text vorhandenen Sprache oder Sprachen	Read			
DetectEntities	Gewährt die Berechtigung, die benannten Entitäten („Personen“, „Orte“, „Standorte“ usw.) im angegebenen Textdokument zu erkennen	Read	entity-recognizer-endpoint		
DetectKeyPhrases	Gewährt die Berechtigung, die Ausdrücke im Text zu erkennen, die in Bezug auf den Inhalt am aussagekräftigsten sind	Read			
DetectPiiEntities	Gewährt die Berechtigung, die persönlich identifizierbaren Informationsentitäten („Name“, „SSN“, „PIN“ usw.) im angegebenen Textdokument zu erkennen	Read			
DetectSentiment	Gewährt die Berechtigung, die Stimmung eines Texts in einem Dokument zu erkennen (positiv, negativ, neutral oder gemischt)	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DetectSyntax	Gewährt die Berechtigung, syntaktische Informationen (wie Wortart, Token) in einem Textdokument zu erkennen	Lesen			
DetectTargetedSentiment	Erteilt die Erlaubnis, die mit bestimmten Entitäten (z. B. Marken oder Produkten) verbundenen Stimmungen innerhalb eines Dokuments zu erkennen	Lesen			
DetectToxicContent	Gewährt die Berechtigung zum Erkennen toxischer Inhalte in der angegebenen Liste von Textsegmenten	Lesen			
ImportModel	Gewährt die Berechtigung zum Importieren eines geschulten Comprehend-Modells	Schreiben	document-classifier*		
			entity-recognizer*		
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:ModelKmsKey	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDatasets	Gewährt die Berechtigung zum Abrufen einer Liste der Datensätze, die einem Flywheel zugeordnet sind	Lesen	flywheel*		
ListDocumentClassificationJobs	Gewährt die Berechtigung zum Abrufen einer Liste der von Ihnen übermittelten Aufträge zur Dokumentklassifizierung	Lesen			
ListDocumentClassifierSummaries	Gewährt die Berechtigung, eine Liste mit Zusammenfassungen der von Ihnen erstellten Dokumentklassifizierer abzurufen	Lesen			
ListDocumentClassifiers	Gewährt die Berechtigung zum Abrufen einer Liste der von Ihnen erstellten Dokumentklassifizierer	Lesen			
ListDominantLanguageDetectionJobs	Gewährt die Berechtigung zum Abrufen einer Liste der dominanten Spracherkennungsaufträge, die Sie übermittelt haben	Lesen			
ListEndpoints	Gewährt die Berechtigung zum Abrufen einer Liste aller vorhandenen Endpunkte, die Sie erstellt haben	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListEntitiesDetectionJobs	Gewährt die Berechtigung zum Abrufen einer Liste der von Ihnen übermittelten Aufträge zur Entitätserkennung	Lesen			
ListEntityRecognizerSummaries	Gewährt die Berechtigung, eine Liste mit Zusammenfassungen für die von Ihnen erstellten Entitätserkenner abzurufen	Lesen			
ListEntityRecognizers	Gewährt die Berechtigung zum Abrufen einer Liste der Eigenschaften aller Entitätserkennungen, die von Ihnen erstellt wurden, einschließlich Erkennungen mit derzeit laufendem Training	Lesen			
ListEventsDetectionJobs	Gewährt die Berechtigung zum Abrufen einer Liste von Ereigniserkennungsaufgaben, die von Ihnen übermittelt wurden	Lesen			
ListFlywheelIterationHistory	Gewährt die Berechtigung zum Abrufen einer Liste der Iterationen, die einem Flywheel zugeordnet sind	Lesen	flywheel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListFlywheels	Gewährt die Berechtigung zum Abrufen einer Liste der von Ihnen erstellten Flywheels	Lesen			
ListKeyPhrasesDetectionJobs	Gewährt die Berechtigung zum Abrufen einer Liste von Schlüsselphrase-Erkennungsaufträgen, die Sie übermittelt haben	Lesen			
ListPiiEntitiesDetectionJobs	Gewährt die Berechtigung zum Abrufen einer Liste der von Ihnen übermittelten Aufträge zur PII-Entitätserkennung	Lesen			
ListSentimentDetectionJobs	Gewährt die Berechtigung zum Abrufen einer Liste der Aufträge zur Stimmungserkennung, die Sie übermittelt haben	Lesen			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen	document-classification-job		
			document-classifier		
			document-classifier-endpoint		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			dominant-language-detection-job		
			entities-detection-job		
			entity-recognizer		
			entity-recognizer-endpoint		
			events-detection-job		
			flywheel		
			flywheel-dataset		
			key-phrases-detection-job		
			pii-entities-detection-job		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			sentiment-detection-job		
			targeted-sentiment-detection-job		
			topics-detection-job		
ListTargetedSentimentDetectionJobs	Gewährt die Berechtigung zum Abrufen einer Liste der Stimmungserkennung saufträge, die Sie abgesendet haben	Lesen			
ListTopicsDetectionJobs	Gewährt die Berechtigung zum Abrufen einer Liste der von Ihnen übermittelten Aufträge zur Themenerkennung	Lesen			
PutResourcePolicy	Gewährt die Berechtigung zum Anfügen einer Richtlinie an eine Ressource	Schreiben	document-classifier*		
			entity-recognizer*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartDocumentClassificationJob	Gewährt die Berechtigung zum Starten eines asynchronen Dokumentklassifizierungsauftrags	Write	document-classification-job*	aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			document-classifier		
			flywheel		
StartDominantLanguageDetectionJob	Gewährt die Berechtigung zum Starten eines asynchronen dominanten Spracherkennungsauftrags für eine Sammlung von Dokumenten	Write	dominant-language-detection-job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartEntitiesDetectionJob	Gewährt die Berechtigung zum Starten eines asynchronen Entitätserkennungsauftrags für eine Sammlung von Dokumenten	Write	entities-detection-job*	aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			entity-recognizer		
			flywheel		
StartEventsDetectionJob	Gewährt die Berechtigung zum Starten einer asynchronen Ereigniserkennungsaufgabe für eine Sammlung von Dokumenten	Schreiben	events-detection-job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:OutputKmsKey	
StartFlywheelIteration	Gewährt die Berechtigung zum Starten einer Flywheel-Iteration	Schreiben	flywheel*		
StartKeyPhrasesDetectionJob	Gewährt die Berechtigung zum Starten eines asynchronen Schlüsselphrase-Erkennungsauftrags für eine Sammlung von Dokumenten	Write	key-phrases-detection-job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
StartPiiEntitiesDetectionJob	Gewährt die Berechtigung zum Starten eines asynchronen Identitätserkennungsauftrags für eine Sammlung von Dokumenten	Write	pii-entities-detection-job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:OutputKmsKey	
StartSentimentDetectionJob	Gewährt die Berechtigung zum Starten eines asynchronen Stimmungserkennung sauftrags für eine Sammlung von Dokumenten	Schreiben	sentiment-detection-job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
StartTargetedSentimentDetectionJob	Gewährt die Berechtigung zum Starten eines asynchronen gezielten Stimmungserkennungsauftrags für eine Sammlung von Dokumenten	Schreiben	targeted-sentiment-detection-job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartTopicsDetectionJob	Gewährt die Berechtigung zum Starten eines asynchronen Auftrags, um die gebräuchlichsten Themen in der Sammlung von Dokumenten sowie die den verschiedenen Themen zugeordneten Ausdrücke zu ermitteln	Write	topics-detection-job*		
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
StopDominantLanguageDetectionJob	Gewährt die Berechtigung zum Beenden eines dominanten Spracherkennungsauftrags	Write	dominant-language-detection-job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopEntitiesDetectionJob	Gewährt die Berechtigung zum Beenden eines Entitätserkennungsauftrags	Write	entities-detection-job*		
StopEventsDetectionJob	Gewährt die Berechtigung zum Beenden einer Ereigniserkennungsaufgabe	Write	events-detection-job*		
StopKeyPhrasesDetectionJob	Gewährt die Berechtigung zum Beenden eines Schlüsselphrase-Erkennungsauftrags	Write	key-phrases-detection-job*		
StopPiiEntitiesDetectionJob	Gewährt die Berechtigung zum Beenden eines PII-Entitätserkennungsauftrags	Write	pii-entities-detection-job*		
StopSentimentDetectionJob	Gewährt die Berechtigung zum Beenden eines Stimmungserkennungsauftrags	Schreiben	sentiment-detection-job*		
StopTargetedSentimentDetectionJob	Gewährt die Berechtigung zum Beenden eines gezielten Stimmungserkennungsauftrags	Schreiben	targeted-sentiment-detection-job*		
StopTrainingDocumentClassifier	Gewährt die Berechtigung, einen zuvor erstellten Trainingsauftrag für einen Dokumentklassifizierer zu beenden	Write	document-classifier*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopTrainingEntityRecognizer	Gewährt die Berechtigung, einen zuvor erstellten Trainingsauftrag für eine Entitätserkennung zu beenden	Write	entity-recognizer*		
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit bestimmten Schlüsselwertpaaren	Markieren	document-classification-job		
			document-classifier		
			document-classifier-endpoint		
			dominant-language-detection-job		
			entities-detection-job		
			entity-recognizer		
			entity-recognizer-endpoint		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			events-detection-job		
			flywheel		
			flywheel-dataset		
			key-phrases-detection-job		
			pii-entities-detection-job		
			sentiment-detection-job		
			targeted-sentiment-detection-job		
			topics-detection-job		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Kennzeichnung einer Ressource mit dem angegebenen Schlüssel	Markieren	document-classification-job		
			document-classifier		
			document-classifier-endpoint		
			dominant-language-detection-job		
			entities-detection-job		
			entity-recognizer		
			entity-recognizer-endpoint		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			events-detection-job		
			flywheel		
			flywheel-dataset		
			key-phrases-detection-job		
			pii-entities-detection-job		
			sentiment-detection-job		
			targeted-sentiment-detection-job		
			topics-detection-job		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateEndpoint	Gewährt die Berechtigung zum Aktualisieren von Informationen über den angegebenen Endpunkt	Schreiben	document-classifier-endpoint*		
			entity-recognizer-endpoint*		
			flywheel		
UpdateFlywheel	Gewährt die Berechtigung zum Aktualisieren einer Flywheel-Konfiguration	Schreiben	flywheel*	comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			document-classifier		
			entity-recognizer		

Von Amazon Comprehend definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
targeted-sentiment-detection-job	`arn:${Partition}:comprehend:${Region}:${Account}:targeted-sentiment-detection-job/${JobId}`	aws:ResourceTag/${TagKey}
document-classifier	`arn:${Partition}:comprehend:${Region}:${Account}:document-classifier/${DocumentClassifierName}`	aws:ResourceTag/${TagKey}
document-classifier-endpoint	`arn:${Partition}:comprehend:${Region}:${Account}:document-classifier-endpoint/${DocumentClassifierEndpointName}`	aws:ResourceTag/${TagKey}
entity-recognizer	`arn:${Partition}:comprehend:${Region}:${Account}:entity-recognizer/${EntityRecognizerName}`	aws:ResourceTag/${TagKey}
entity-recognizer-endpoint	`arn:${Partition}:comprehend:${Region}:${Account}:entity-recognizer-endpoint/${EntityRecognizerEndpointName}`	aws:ResourceTag/${TagKey}
dominant-language-detection-job	`arn:${Partition}:comprehend:${Region}:${Account}:dominant-language-detection-job/${JobId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
entities-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:entities-detection-job/${JobId}	aws:ResourceTag/${TagKey}
pii-entities-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:pii-entities-detection-job/${JobId}	aws:ResourceTag/${TagKey}
events-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:events-detection-job/${JobId}	aws:ResourceTag/${TagKey}
key-phrases-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:key-phrases-detection-job/${JobId}	aws:ResourceTag/${TagKey}
sentiment-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:sentiment-detection-job/${JobId}	aws:ResourceTag/${TagKey}
topics-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:topics-detection-job/${JobId}	aws:ResourceTag/${TagKey}
document-classification-job	arn:${Partition}:comprehend:${Region}:${Account}:document-classification-job/${JobId}	aws:ResourceTag/${TagKey}
flywheel	arn:${Partition}:comprehend:${Region}:${Account}:flywheel/${FlywheelName}	aws:ResourceTag/${TagKey}
flywheel-dataset	arn:${Partition}:comprehend:${Region}:${Account}:flywheel/${FlywheelName}/dataset/${DatasetName}	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Comprehend

Amazon Comprehend definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff, mit Tag-Werten, die in der Anforderung zur Ressourcenerstellung erforderlich sind	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff, mit einem Tag-Wert, der der Ressource zugeordnet sein muss	Zeichenfolge
aws:TagKeys	Filtert den Zugriff, indem verbindliche Tags in der Anforderung vorhanden sein müssen	ArrayOfString
comprehend:DataLakeKmsKey	Filtert den Zugriff nach dem DataLake-KMS-Schlüssel, der der Flywheel-Ressource in der Anforderung zugeordnet ist	ARN
comprehend:FlywheelIterationId	Filtert den Zugriff nach einer bestimmten Iterations-ID für ein Flywheel	Zeichenfolge
comprehend:ModelKmsKey	Filtert den Zugriff durch den KMS-Modellschlüssel, der der Ressource in der Anforderung zugeordnet ist	ARN
comprehend:OutputKmsKey	Filtert den Zugriff durch den KMS-Ausgabeschlüssel, der der Ressource in der Anforderung zugeordnet ist	ARN

Bedingungsschlüssel	Beschreibung	Typ
comprehend:VolumeKmsKey	Filtert den Zugriff durch den KMS-Volume-Schlüssel, der der Ressource in der Anforderung zugeordnet ist	ARN
comprehend:VpcSecurityGroupIds	Filtert den Zugriff über die Liste aller VPC-Sicherheitsgruppen-IDs, die der Ressource in der Anforderung zugeordnet sind	ArrayOfString
comprehend:VpcSubnets	Filtert den Zugriff über die Liste aller VPC-Subnetze, die der Ressource in der Anforderung zugeordnet sind	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Comprehend Medical

Amazon Comprehend Medical (Servicepräfix: `comprehendmedical`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Comprehend Medical definierte Aktionen
- Von Amazon Comprehend Medical definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Comprehend Medical

Von Amazon Comprehend Medical definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeEntitiesDetectionV2Job	Gewährt die Berechtigung, die Eigenschaften einer von Ihnen übermittelten medizinischen Entitätserkennungsaufgabe zu beschreiben	Read			
DescribeICD10CMInferenceJob	Gewährt die Berechtigung, die Eigenschaften einer ICD-10-CM-Verknüpfungsaufgabe zu beschreiben, die Sie eingereicht haben	Read			
DescribePHIDetectionJob	Gewährt die Berechtigung zur Beschreibung der Eigenschaften einer von Ihnen übermittelten Aufgabe zur PHI-Entitätserkennung	Read			
DescribeRxNormInferenceJob	Gewährt die Berechtigung, die Eigenschaften einer RxNorm-Verknüpfungsaufgabe zu beschreiben, die Sie übermittelt haben	Lesen			
DescribeSNOMEDCTInferenceJob	Gewährt die Berechtigung, die Eigenschaften einer SNOMED-CT-Verknüpfungsaufgabe zu beschreiben, die Sie übermittelt haben	Lesen			
DetectEntitiesV2	Gewährt die Berechtigung, die benannten medizinischen Entitäten und ihre	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Beziehungen und Eigenschaften innerhalb des gegebenen Textdokuments zu erkennen				
DetectPHI	Gewährt die Berechtigung, die geschützten Gesundheitsinformationen (PHI) innerhalb des gegebenen Textdokuments zu erkennen	Read			
InferICD10CM	Gewährt die Berechtigung, die Gesundheitszustands-Entitäten innerhalb des gegebenen Textdokuments zu erkennen und sie mit ICD-10-CM-Codes zu verknüpfen	Read			
InferRxNorm	Gewährt die Berechtigung, die Medikamente innerhalb des gegebenen Textdokuments zu erkennen und sie mit RxCUI-Konzeptkennungen aus der National-Library-of-Medicine-RxNorm-Datenbank zu verknüpfen	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
InferSNOMEDCT	Gewährt die Berechtigung, den Gesundheitszustand, die Anatomie sowie die Test-, Behandlungs- und Verfahrens-Entitäten im gegebenen Textdokument zu erkennen und sie mit SNOMED-CT-Codes zu verknüpfen	Lesen			
ListEntitiesDetectionV2Jobs	Gewährt die Berechtigung zum Auflisten der von Ihnen übermittelten Aufgaben zur medizinischen Entitätserkennung	Read			
ListICD10CMInferenceJobs	Gewährt die Berechtigung zum Auflisten der von Ihnen übermittelten ICD-10-CM-Verknüpfungsaufgaben	Read			
ListPHIDetectionJobs	Gewährt die Berechtigung zum Auflisten der von Ihnen übermittelten Aufträge zur PHI-Entitätserkennung	Read			
ListRxNormInferenceJobs	Gewährt die Berechtigung zum Auflisten der von Ihnen übermittelten RxNorm-Verknüpfungsaufgaben	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListSNOMEDCTInferenceJobs	Gewährt die Berechtigung zum Auflisten der von Ihnen übermittelten SNOMED-CT-Verknüpfungsaufgaben	Lesen			
StartEntitiesDetectionV2Job	Gewährt die Berechtigung zum Starten eines asynchronen medizinischen Entitätserkennungsauftrags für eine Sammlung von Dokumenten	Write			
StartICD10CMInferenceJob	Gewährt die Berechtigung zum Starten einer asynchronen ICD-10-CM-Verknüpfungsaufgabe für eine Sammlung von Dokumenten	Write			
StartPHIDetectionJob	Gewährt die Berechtigung zum Starten eines asynchronen PHI-Entitätserkennungsauftrags für eine Sammlung von Dokumenten	Write			
StartRxNormInferenceJob	Gewährt die Berechtigung zum Starten einer asynchronen RxNorm-Verknüpfungsaufgabe für eine Sammlung von Dokumenten	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartSNOMEDCTInferenceJob	Gewährt die Berechtigung zum Starten einer asynchronen SNOMED-CT-Verknüpfungsaufgabe für eine Sammlung von Dokumenten	Schreiben			
StopEntitiesDetectionV2Job	Gewährt die Berechtigung zum Beenden einer medizinischen Entitätserkennungsaufgabe	Write			
StopICD10CMInferenceJob	Gewährt die Berechtigung, eine ICD-10-CM-Verknüpfungsaufgabe zu stoppen	Write			
StopPHIDetectionJob	Gewährt die Berechtigung zum Beenden einer PHI-Entitätserkennungsaufgabe	Write			
StopRxNormInferenceJob	Gewährt die Berechtigung zum Stoppen einer RxNorm-Verknüpfungsaufgabe	Schreiben			
StopSNOMEDCTInferenceJob	Gewährt die Berechtigung, eine SNOMED-CT-Verknüpfungsaufgabe zu stoppen	Schreiben			

Von Amazon Comprehend Medical definierte Ressourcentypen

Amazon Comprehend Medical unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf Amazon Comprehend Medical zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für Amazon Comprehend Medical

Amazon Comprehend Medical definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Compute Optimizer

AWS Compute Optimizer (Servicepräfix: `compute-optimizer`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Vom AWS Compute Optimizer definierte Aktionen
- Von AWS Compute Optimizer definierte Ressourcentypen
- Bedingungsschlüssel für AWS Compute Optimizer

Vom AWS Compute Optimizer definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteRecommendationPreferences	Gewährt die Berechtigung zum Löschen von Empfehlungseinstellungen	Schreiben		compute-optimizer:ResourceType	autoscaling:DescribeAutoScalingGroups ec2:DescribeInstances
DescribeRecommendationExportJobs	Gewährt die Berechtigung zum Anzeigen des Status von Empfehlungsexportaufgaben	Auflisten			
ExportAutoScalingGroupRecommendations	Gewährt die Berechtigung zum Exportieren von Auto-Scaling-Gruppen-Empfehlungen in S3 für die bereitgestellten Konten	Schreiben			autoscaling:DescribeAutoScalingGroups compute-optimizer:GetAutoScalingGroupRecommendations
ExportEBSVolumeRecommendations	Gewährt die Berechtigung zum Exportieren von EBS-Volume-Empfehlungen in S3 für die bereitgestellten Konten	Schreiben			compute-optimizer:GetEBSVolumeRecommendations

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ec2:DescribeVolumes
ExportEC2InstanceRecommendations	Gewährt die Berechtigung zum Exportieren von EC2-Instance-Empfehlungen in S3 für die bereitgestellten Konten	Schreiben			compute-optimizer:GetEC2InstanceRecommendations ec2:DescribeInstances
ExportECSServiceRecommendations	Gewährt die Berechtigung zum Exportieren von EBS-Serviceempfehlungen in S3 für die bereitgestellten Konten	Schreiben			compute-optimizer:GetECSServiceRecommendations ecs:ListClusters ecs:ListServices

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ExportLambdaFunctionRecommendations	Gewährt die Berechtigung zum Exportieren von Lambda-Funktion-Empfehlungen in S3 für die bereitgestellten Konten	Schreiben			compute-optimizer:GetLambdaFunctionRecommendations lambda:ListFunctions lambda:ListProvisionedConcurrencyConfigs
ExportLicenseRecommendations	Gewährt die Berechtigung zum Exportieren von Lizenzempfehlungen in S3 für angegebene Konten	Schreiben			compute-optimizer:GetLicenseRecommendations ec2:DescribeInstances
GetAutoScalingGroupRecommendations	Gewährt die Berechtigung zum Abrufen von Empfehlungen für die bereitgestellten Auto-Scaling-Gruppen	Auflisten			autoscaling:DescribeAutoScalingGroups

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetEBSVolumeRecommendations	Gewährt die Berechtigung zum Abrufen von Empfehlungen für die bereitgestellten EBS-Volumes	Auflisten			ec2:DescribeVolumes
GetEC2InstanceRecommendations	Gewährt die Berechtigung zum Abrufen von Empfehlungen für die bereitgestellten EC2-Instances	Auflisten			ec2:DescribeInstances
GetEC2RecommendationProjectedMetrics	Gewährt die Berechtigung zum Abrufen der prognostizierten Empfehlungsmetriken der angegebenen Instance	Auflisten			ec2:DescribeInstances
GetECSServiceRecommendationProjectedMetrics	Gewährt die Berechtigung zum Abrufen der prognostizierten Empfehlungsmetriken des angegebenen ECS-Services	Auflisten			
GetECSServiceRecommendations	Gewährt die Berechtigung zum Abrufen von Empfehlungen für die bereitgestellten ECS-Services	Auflisten			ecs:ListClusters ecs:ListServices

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetEffectiveRecommendationPreferences	Gewährt die Berechtigung zum Abrufen von aktiven Empfehlungseinstellungen	Lesen		compute-optimizer:ResourceType	autoscaling:DescribeAutoScalingGroups autoscaling:DescribeAutoScalingInstances ec2:DescribeInstances
GetEnrollmentStatus	Gewährt die Berechtigung zum Abrufen des Registrierungsstatus für das angegebene Konto	Auflisten			
GetEnrollmentStatusesForOrganization	Gewährt die Berechtigung zum Abrufen des Registrierungsstatus für Mitgliedskonten der Organisation	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetLambdaFunctionRecommendations	Gewährt die Berechtigung zum Abrufen von Empfehlungen für die bereitgestellten Lambda-Funktionen	Auflisten			lambda:ListFunctions lambda:ListProvisionedConcurrencyConfigs
GetLicenseRecommendations	Gewährt die Berechtigung zum Abrufen von Lizenzempfehlungen für angegebene Konten	Auflisten			ec2:DescribeInstances
GetRecommendationPreferences	Gewährt die Berechtigung zum Abrufen von Empfehlungseinstellungen	Lesen		compute-optimizer:ResourceType	
GetRecommendationSummaries	Gewährt die Berechtigung zum Abrufen der Empfehlungszusammenfassungen für die angegebenen Konten	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutRecommendationPreferences	Gewährt die Berechtigung zum Ablegen von Empfehlungseinstellungen	Schreiben		compute-optimizer:ResourceType	autoscaling:DescribeAutoScalingGroups autoscaling:DescribeAutoScalingInstances ec2:DescribeInstances
UpdateEnrollmentStatus	Gewährt die Berechtigung zum Aktualisieren des Registrierungsstatus	Schreiben			

Von AWS Compute Optimizer definierte Ressourcentypen

AWS Compute Optimizer unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf AWS Compute Optimizer zu ermöglichen, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Compute Optimizer

AWS Compute Optimizer definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
compute-optimizer:ResourceType	Filtert den Zugriff nach dem Ressourcen-Typ	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Config

AWS Config (Servicepräfix: `config`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Config definierte Aktionen
- Von AWS Config definierte Ressourcentypen
- Bedingungsschlüssel für AWS Config

Von AWS Config definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetAggregateResourceConfig	Gewährt die Berechtigung, die aktuellen Konfigurationselemente für Ressourcen in Ihrem	Read	ConfigurationAggregator*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	AWS-Config-Aggregator zurückzugeben				
BatchGetResourceConfig	Gewährt die Berechtigung, die aktuelle Konfiguration für eine oder mehrere angeforderte Ressourcen zurückzugeben	Read			
DeleteAggregationAuthorization	Gewährt die Berechtigung zum Löschen der Autorisierung, die dem angegebenen Konfigurationsaggregatorkonto in einer bestimmten Region gewährt wurde	Write	AggregationAuthorization*		
DeleteConfigRule	Gewährt die Berechtigung zum Löschen der angegebenen AWS-Config-Regel und aller zugehörigen Auswertungsergebnisse	Write	ConfigRule*		
DeleteConfigurationAggregator	Gewährt die Berechtigung, den angegebenen Konfigurationsaggregator und die mit dem Aggregator verknüpften zusammengeführten Daten zu löschen	Write	ConfigurationAggregator*		
DeleteConfigurationRecorder	Gewährt die Berechtigung zum Löschen des Configuration Recorder	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteConformancePack	Gewährt die Berechtigung, das angegebene Compliancepaket sowie alle AWS-Config-Regeln und Auswertungsergebnisse innerhalb dieses Compliancepakets zu löschen	Write	ConformancePack*		
DeleteDeliveryChannel	Gewährt die Berechtigung zum Löschen des Bereitstellungskanals	Write			
DeleteEvaluationResults	Gewährt die Berechtigung zum Löschen der Auswertungsergebnisse für die angegebene Config-Regel	Write	ConfigRule*		
DeleteOrganizationConfigRule	Gewährt die Berechtigung, die angegebene Organisationskonfigurationsregel und alle zugehörigen Auswertungsergebnisse aus allen Mitgliedskonten der Organisation zu löschen	Write	OrganizationConfigRule*		
DeleteOrganizationConformancePack	Gewährt die Berechtigung, das angegebene Organisationskonformitätspaket und alle zugehörigen Auswertungsergebnisse aus allen Mitgliedskonten der Organisation zu löschen	Write	OrganizationConformancePack*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeletePendingAggregationRequest	Gewährt die Berechtigung, ausstehende Autorisierungsanforderungen für ein bestimmtes Aggregatorkonto in einer bestimmten Region zu löschen	Write			
DeleteRemediationConfiguration	Gewährt die Berechtigung zum Löschen der Korrektur konfiguration	Write	RemediationConfiguration*		
DeleteRemediationExceptions	Gewährt die Berechtigung, eine oder mehrere Korrektur ausnahmen für bestimmte Ressourcenschlüssel einer bestimmten AWS-Config-Regel zu löschen	Write			
DeleteResourceConfig	Gewährt die Berechtigung, den Konfigurationsstatus einer benutzerdefinierten Ressource aufzuzeichnen, die gelöscht wurde	Write			
DeleteRetentionConfiguration	Gewährt die Berechtigung zum Löschen der Aufbewahrungskonfiguration	Write			
DeleteStoredQuery	Gewährt die Berechtigung zum Löschen der gespeicherten Abfrage für ein AWS-Konto in einer AWS-Region	Write	StoredQuery*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeliverConfigSnapshot	Gewährt die Berechtigung, die Übermittlung eines Konfigurations-Snapshots an den Amazon-S3-Bucket über den angegebenen Bereitstellungskanal zu planen	Read			
DescribeAggregateComplianceByConfigRules	Gewährt die Berechtigung, eine Liste der konformen und nicht konformen Regeln mit der Anzahl der Ressourcen für konforme und nicht konforme Regeln zurückzugeben	Read	ConfigurationAggregator*		
DescribeAggregateComplianceByConformancePacks	Gewährt die Berechtigung, eine Liste von konformen und nicht konformen Compliancepaketen zusammen mit der Anzahl der konformen, nicht konformen und Gesamtregeln in jedem Compliancepaket zurückzugeben	Read	ConfigurationAggregator*		
DescribeAggregationAuthorizations	Gewährt die Berechtigung, eine Liste der Autorisierungen für verschiedene Aggregatorkonten und -regionen zurückzugeben	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeComplianceByConfigRule	Gewährt die Berechtigung, anzugeben, ob die angegebenen AWS-Config-Regeln konform sind	Read			
DescribeComplianceByResource	Gewährt die Berechtigung, anzugeben, ob die angegebenen AWS-Ressourcen konform sind	Read			
DescribeConfigRuleEvaluationStatus	Gewährt die Berechtigung, Statusinformationen für jede Ihrer AWS-verwalteten Config-Regeln zurückzugeben	Read			
DescribeConfigRules	Gewährt die Berechtigung, Details zu Ihren AWS-Config-Regeln zurückzugeben	List			
DescribeConfigurationAggregatorSourcesStatus	Gewährt die Berechtigung, Statusinformationen für Quellen innerhalb eines Aggregators zurückzugeben	Read	ConfigurationAggregator*		
DescribeConfigurationAggregators	Gewährt die Berechtigung, die Details eines oder mehrerer Konfigurationsaggregatoren zurückzugeben	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeConfigurationRecorderStatus	Gewährt die Berechtigung, den aktuellen Status des angegebenen Configuration Recorder zurückzugeben	Read			
DescribeConfigurationRecorders	Gewährt die Berechtigung, die Namen eines oder mehrerer angegebener Configuration Recorder zurückzugeben	List			
DescribeConformancePackCompliance	Gewährt die Berechtigung, Compliance-Informationen für jede Regel in diesem Compliancepaket zurückzugeben	Read	ConformancePack*		
DescribeConformancePackStatus	Gewährt die Berechtigung, den Bereitstellungsstatus eines oder mehrerer Compliancepakete bereitzustellen	Read			
DescribeConformancePacks	Gewährt die Berechtigung, eine Liste eines oder mehrerer Compliancepakete zurückzugeben	List			
DescribeDeliveryChannelStatus	Gewährt die Berechtigung, den aktuellen Status des angegebenen Bereitstellungskanals zurückzugeben	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDeliveryChannels	Gewährt die Berechtigung, Details zum angegebenen Bereitstellungskanal zurückzugeben	List			
DescribeOrganizationConfigRuleStatuses	Gewährt die Berechtigung, den Bereitstellungsstatus von Organisationskonfigurationsregeln für eine Organisation bereitzustellen	Read			
DescribeOrganizationConfigRules	Gewährt die Berechtigung, eine Liste von Organisationskonfigurationsregeln zurückzugeben	List			
DescribeOrganizationConformancePackStatuses	Gewährt die Berechtigung, den Bereitstellungsstatus des Compliancepakets für eine Organisation bereitzustellen	Read			
DescribeOrganizationConformancePacks	Gewährt die Berechtigung, eine Liste von Organisationskonformitätspaketen zurückzugeben	List			
DescribePendingAggregationRequests	Gewährt die Berechtigung, eine Liste aller ausstehenden Aggregationsanforderungen zurückzugeben	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeRemediationConfigurations	Gewährt die Berechtigung, die Details einer oder mehrerer Korrekturkonfigurationen zurückzugeben	List	RemediationConfiguration*		
DescribeRemediationExceptions	Gewährt die Berechtigung, die Details einer oder mehrerer Korrekturausnahmen zurückzugeben	List			
DescribeRemediationExecutionStatus	Gewährt die Berechtigung, eine detaillierte Ansicht einer Korrekturausführung für eine Reihe von Ressourcen bereitzustellen, einschließlich Status, Zeitstempel und Fehlermeldungen für fehlgeschlagene Schritte	Read	RemediationConfiguration*		
DescribeRetentionConfigurations	Gewährt die Berechtigung, die Details einer oder mehrerer Aufbewahrungskonfigurationen zurückzugeben	List			
GetAggregateComplianceDetailsByConfigRule	Gewährt die Berechtigung, die Auswertungsergebnisse für die angegebene AWS-Config-Regel für eine bestimmte Ressource in einer Regel zurückzugeben	Read	ConfigurationAggregator*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAggregateConfigRuleComplianceSummary	Gewährt die Berechtigung, die Anzahl der konformen und nicht konformen Regeln für ein oder mehrere Konten und Regionen in einem Aggregator zurückzugeben	Read	ConfigurationAggregator*		
GetAggregateConformancePackComplianceSummary	Gewährt die Berechtigung, die Anzahl der konformen und nicht konformen Compliancepakete für ein oder mehrere Konten und Regionen in einem Aggregator zurückzugeben	Read	ConfigurationAggregator*		
GetAggregateDiscoveredResourceCounts	Gewährt die Berechtigung, die Ressourcenanzahl für die Konten und Regionen in Ihrem AWS-Config-Aggregator zurückzugeben	Read	ConfigurationAggregator*		
GetAggregateResourceConfig	Gewährt die Berechtigung, das Konfigurationselement zurückzugeben, das für Ihre Ressource in einem bestimmten Quellkonto und einer bestimmten Region aggregiert ist	Read	ConfigurationAggregator*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetComplianceDetailsByConfigRule	Gewährt die Berechtigung, die Auswertungsergebnisse für die angegebene AWS-Config-Regel zurückzugeben	Read	ConfigRule*		
GetComplianceDetailsByResource	Gewährt die Berechtigung, die Auswertungsergebnisse für die angegebene AWS-Ressource zurückzugeben	Read			
GetComplianceSummaryByConfigRule	Gewährt die Berechtigung, die Anzahl der AWS-Config-Regeln zurückzugeben, die konform und nicht konform sind (jeweils maximal 25)	Read			
GetComplianceSummaryByResourceType	Gewährt die Berechtigung, die Anzahl der Ressourcen zurückzugeben, die konform und nicht konform sind	Read			
GetConformancePackComplianceDetails	Gewährt die Berechtigung, die Compliance-Details eines Compliancepakets für alle AWS-Ressourcen zurückzugeben, die vom Compliancepaket überwacht werden	Read	ConformancePack*		
GetConformancePackComplianceSummary	Gewährt die Berechtigung, eine Complianceübersicht für ein oder mehrere Compliancepakete bereitzustellen	Lesen	ConformancePack*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetCustomRulePolicy	Gewährt die Berechtigung zum Zurückgeben der Richtliniendefinition, die die Logik für die Regel der benutzerdefinierten AWS-Konfigurationsrichtlinie enthält	Lesen	ConfigRule*		
GetDiscoveredResourceCounts	Gewährt die Berechtigung, die Ressourcentypen, die Anzahl der einzelnen Ressourcentypen und die Gesamtzahl der Ressourcen zurückzugeben, die AWS Config in dieser Region für Ihr AWS-Konto aufzeichnet	Read			
GetOrganizationConfigRuleDetailedStatus	Gewährt die Berechtigung, den detaillierten Status jedes Mitgliedskontos innerhalb einer Organisation für eine Organisationskonfigurationsregel zurückzugeben	Read	OrganizationConfigRule*		
GetOrganizationConformancePackDetailedStatus	Gewährt die Berechtigung, den detaillierten Status jedes Mitgliedskontos innerhalb einer Organisation für ein bestimmtes Organisationskonformitätspaket zurückzugeben	Lesen	OrganizationConformancePack*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetOrganizationCustomRulePolicy	Gewährt die Berechtigung zum Zurückgeben der Richtlinendefinition, die die Logik für die Regel der benutzerdefinierten AWS-Konfigurationsrichtlinie Ihrer Organisation enthält	Lesen	OrganizationConfigRule*		
GetResourceConfigHistory	Gewährt die Berechtigung, eine Liste von Konfigurationselementen für die angegebene Ressource zurückzugeben	Lesen			
GetResourceEvaluationSummary	Gewährt die Berechtigung zum Zurückgeben der Zusammenfassung der Auswertungsergebnisse für eine bestimmte Ressourcenauswertungs-ID	Lesen			
GetStoredQuery	Gewährt die Berechtigung, die Details einer bestimmten gespeicherten Abfrage zurückzugeben	Read	StoredQuery*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAggregateDiscoveredResources	Gewährt die Berechtigung, einen Ressourcentyp zu akzeptieren und eine Liste der Ressourcen-IDs zurückzugeben, die für einen bestimmten Ressourcentyp in verschiedenen Konten und Regionen aggregiert werden	Auflisten	ConfigurationAggregator*		
ListConformancePackComplianceScores	Gewährt die Berechtigung zum Zurückgeben des Prozentsatzes konformer Regel-Ressourcen-Kombinationen in einem Conformance Pack im Vergleich zur Anzahl aller möglichen Regel-Ressourcen-Kombinationen	Auflisten			
ListDiscoveredResources	Gewährt die Berechtigung, einen Ressourcentyp zu akzeptieren und eine Liste der Ressourcen-IDs für die Ressourcen dieses Typs zurückzugeben	Auflisten			
ListResourceEvaluations	Gewährt die Berechtigung zum Auflisten der Zusammenfassungen der Ressourcenauswertung für ein AWS-Konto in einer AWS-Region	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListStoredQueries	Gewährt die Berechtigung zum Auflisten der gespeicherten Abfragen für ein AWS-Konto in einer AWS-Region	List			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für eine AWS-Config-Ressource	Read	AggregationAuthorization		
			ConfigRule		
			ConfigurationAggregator		
			ConformancePack		
			OrganizationConfigRule		
			OrganizationConformancePack		
			StoredQuery		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutAggregationAuthorization	Gewährt die Berechtigung, das Aggregatorkonto und die Region dazu zu autorisieren, Daten aus dem Quellkonto und der Quellregion zu erfassen	Write	AggregationAuthorization*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutConfigRule	Gewährt die Berechtigung, eine AWS-Config-Regel hinzuzufügen oder zu aktualisieren, um zu prüfen, ob Ihre AWS-Ressourcen den gewünschten Konfigurationen entsprechen	Write	ConfigRule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutConfigurationAggregator	Gewährt die Berechtigung, den Konfigurationsaggregator mit den ausgewählten Quellkonten und -regionen zu erstellen und zu aktualisieren	Write	ConfigurationAggregator*		iam:PassRole organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
PutConfigurationRecorder	Gewährt die Berechtigung, einen neuen Configuration Recorder zur Aufzeichnung der ausgewählten Ressourcenkonfigurationen zu erstellen	Write			
PutConformancePack	Gewährt die Berechtigung zum Erstellen oder Aktualisieren eines Compliancepakets	Write	ConformancePack*		iam:CreateServiceLinkedRole iam:PassRole s3:GetObject s3:ListBucket ssm:GetDocument

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutDeliveryChannel	Gewährt die Berechtigung, ein Bereitstellungskanalobjekt zu erstellen, um Konfigurationsinformationen in einem Amazon-S3-Bucket und einem Amazon SNS-Thema bereitzustellen	Write			
PutEvaluations	Gewährt die Berechtigung, um zur Bereitstellung der Auswertungsergebnisse in AWS Config von einer AWS-Lambda-Funktion verwendet zu werden	Write			
PutExternalEvaluation	Gewährt die Berechtigung, das Auswertungsergebnis in AWS Config bereitzustellen	Write	ConfigRule*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutOrganizationConfigRule	Gewährt die Berechtigung, eine Organisationskonfigurationsregel für Ihre gesamte Organisation hinzuzufügen oder zu aktualisieren, um zu bewerten, ob Ihre AWS-Ressourcen den gewünschten Konfigurationen entsprechen	Write	OrganizationConfigRule*		iam:CreateServiceLinkedRole iam:PassRole organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutOrganizationConformancePack	Gewährt die Berechtigung, ein Organisationskonformitätspaket für Ihre gesamte Organisation hinzuzufügen oder zu aktualisieren, um zu bewerten, ob Ihre AWS-Ressourcen den gewünschten Konfigurationen entsprechen	Write	OrganizationConformancePack*		iam:CreateServiceLinkedRole iam:PassRole organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators s3:GetObject
PutRemediationConfigurations	Gewährt die Berechtigung, die Korrekturkonfiguration mit einer bestimmten AWS-Config-Regel und dem ausgewählten Ziel oder der ausgewählten Aktion zu ergänzen oder zu aktualisieren	Write	RemediationConfiguration*		iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutRemediationExceptions	Gewährt die Berechtigung, Korrekturausnahmen für bestimmte Ressourcen für eine bestimmte AWS-Config-Regel hinzuzufügen oder zu aktualisieren	Write			
PutResourceConfig	Gewährt die Berechtigung, den Konfigurationsstatus für die in der Anforderung bereitgestellte Ressource aufzuzeichnen	Write			
PutRetentionConfiguration	Gewährt die Berechtigung, die Aufbewahrungskonfiguration, in der AWS Config Ihre Verlaufsinformationen speichert, mit Details zur Aufbewahrungsfrist (Anzahl der Tage) zu erstellen und zu aktualisieren	Write			
PutStoredQuery	Gewährt die Berechtigung, eine neue Abfrage zu speichern oder eine vorhandene gespeicherte Abfrage zu aktualisieren	Write	StoredQuery*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SelectAggregateResourceConfig	Gewährt die Berechtigung, einen SQL-SELECT-Befehl und einen Aggregator zu akzeptieren, um den Konfigurationsstatus von AWS-Ressourcen in verschiedenen Konten und Regionen abzufragen, die entsprechende Suche durchzuführen und Ressourcenkonfigurationen zurückzugeben, die den Eigenschaften entsprechen	Read	ConfigurationAggregator*		
SelectResourceConfig	Gewährt die Berechtigung, einen SQL-SELECT-Befehl zu akzeptieren, die entsprechende Suche durchzuführen und Ressourcenkonfigurationen zurückzugeben, die den Eigenschaften entsprechen	Read			
StartConfigRulesEvaluation	Gewährt die Berechtigung zur Bewertung Ihrer Ressourcen anhand der angegebenen Config-Regeln	Write	ConfigRule*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartConfigurationRecorder	Gewährt die Berechtigung, die Aufzeichnung von Konfigurationen der AWS-Ressourcen zu starten, die Sie in Ihrem AWS-Konto für die Aufzeichnung ausgewählt haben	Write			
StartRemediationExecution	Gewährt die Berechtigung, eine On-Demand-Korrektur für die angegebenen AWS-Config-Regeln mithilfe der letzten bekannten Korrekturkonfiguration auszuführen	Schreiben			iam:PassRole
StartResourceEvaluation	Gewährt die Berechtigung zum Bewerten Ihrer Ressourcendetails anhand der AWS-Config-Regeln in Ihrem Konto	Schreiben			cloudformation:DescribeType
StopConfigurationRecorder	Gewährt die Berechtigung, die Aufzeichnung von Konfigurationen der AWS-Ressourcen zu beenden, die Sie in Ihrem AWS-Konto für die Aufzeichnung ausgewählt haben	Write			
TagResource	Gewährt die Berechtigung, die angegebenen Tags einer Ressource mit der angegebenen Ressource zuzuordnen	Markieren	AggregationAuthorization		
			ConfigRule		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			ConfigurationAggregator		
			ConformancePack		
			OrganizationConfigRule		
			OrganizationConformancePack		
			StoredQuery		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Löschen eines oder mehrerer Tags aus einer Ressource	Markieren	AggregationAuthorization		
			ConfigRule		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			ConfigurationAggregator		
			ConformancePack		
			OrganizationConfigRule		
			OrganizationConformancePack		
			StoredQuery		
				aws:TagKeys	

Von AWS Config definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
AggregationAuthorization	arn:${Partition}:config:${Region}:${Account}:aggregation-authorization/${AggregatorAccount}/${AggregatorRegion}	aws:ResourceTag/${TagKey}
ConfigurationAggregator	arn:${Partition}:config:${Region}:${Account}:config-aggregator/${AggregatorId}	aws:ResourceTag/${TagKey}
ConfigRule	arn:${Partition}:config:${Region}:${Account}:config-rule/${ConfigRuleId}	aws:ResourceTag/${TagKey}
ConformancePack	arn:${Partition}:config:${Region}:${Account}:conformance-pack/${ConformancePackName}/${ConformancePackId}	aws:ResourceTag/${TagKey}
OrganizationConfigRule	arn:${Partition}:config:${Region}:${Account}:organization-config-rule/${OrganizationConfigRuleId}	aws:ResourceTag/${TagKey}
OrganizationConformancePack	arn:${Partition}:config:${Region}:${Account}:organization-conformance-pack/${OrganizationConformancePackId}	aws:ResourceTag/${TagKey}
RemediationConfiguration	arn:${Partition}:config:${Region}:${Account}:remediation-configuration/${RemediationConfigurationId}	
StoredQuery	arn:${Partition}:config:${Region}:${Account}:stored-query/${StoredQueryName}/${StoredQueryId}	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Config

AWS Config definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den zulässigen Werten für jeden der Tags	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Tag-Wert, der der Ressource zugeordnet ist	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach dem Vorhandensein verbindlicher Tags in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Connect

Amazon Connect (Servicepräfix: `connect`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Connect definierte Aktionen

- Von Amazon Connect definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Connect

Von Amazon Connect definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ActivateEvaluationForm	Gewährt die Berechtigung zum Aktivieren eines Evaluierungsformulars in der angegebenen Amazon-Connect-Instance. Nach seiner Aktivierung kann das Evaluierungsformular zum Starten neuer Evaluierungen verwendet werden	Schreiben	evaluation-form*		
				connect:InstanceId	
AdminGetEmergencyAccessToken	Gewährt die Berechtigung zum Verbund in eine Amazon-Connect-Instance (Melden Sie sich für die Notfallzugriff-Funktion in der Amazon-Connect-Konsole an)	Schreiben	instance*		connect:DescribeInstance connect:ListInstances ds:DescribeDirectories
AssociateApprovedOrigin	Gewährt Berechtigungen zum Zuordnen des genehmigten Ursprungs für eine bestehende Amazon-Connect-Instance	Schreiben	instance*		
				connect:InstanceId	
AssociateBot	Gewährt Berechtigungen zum Zuordnen eines Lex-Bots für eine bestehende Amazon-Connect-Instance	Schreiben	instance*		iam:AttachRolePolicy

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					iam:CreateServiceLinkedRole iam:PutRolePolicy lex:CreateResourcePolicy lex:DescribeBotAlias lex:GetBot lex:UpdateResourcePolicy
				connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Associate CustomerProfilesDomain [nur Berechtigung]	Gewährt Berechtigungen zum Zuordnen einer Customer-Profiles-Domain für eine vorhandene Amazon-Connect-Instance	Schreiben	instance*		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy profile:GetDomain
Associate DefaultVocabulary	Gewährt die Berechtigung zum Standardvokabular für eine vorhandene Amazon Connect-Instance	Schreiben	instance*		
				connect:InstanceId	
Associate Flow	Gewährt die Berechtigung zum Zuordnen einer Ressource mit einem Gesprächsablauf in einer Amazon-Connect-Instance	Schreiben	contact-flow*		
			instance*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateInstanceStorageConfig	Gewährt Berechtigungen zum Zuordnen des Instance-Speichers für eine bestehende Amazon-Connect-Instance	Schreiben	instance*		ds:DescribeDirectories firehose:DescribeDeliveryStream iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy kinesis:DescribeStream kms:CreateGrant kms:DescribeKey s3:GetBucketAcl

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					s3:GetBucketLocation
				connect:StorageResourceType connect:InstanceId	
Associate LambdaFunction	Gewährt Berechtigungen zum Zuordnen einer Lambda-Funktion für eine bestehende Amazon-Connect-Instance	Schreiben	instance*		lambda:AddPermission
				connect:InstanceId	
Associate LexBot	Gewährt Berechtigungen zum Zuordnen eines Lex-Bots für eine bestehende Amazon-Connect-Instance	Schreiben	instance*		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy lex:GetBot
				connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociatePhoneNumberContactFlow	Gewährt die Berechtigung zum Zuordnen von Gesprächsablauf-Ressourcen zu Telefonnummern in einer Amazon-Connect-Instance	Schreiben	contact-flow*		
			phone-number*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
AssociateQueueQuickConnects	Gewährt Berechtigungen zum Zuordnen von Schnellverbindern mit einer Warteschlange in einer Amazon-Connect-Instance	Schreiben	queue*		
			quick-connect*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
AssociateRoutingProfileQueues	Gewährt Berechtigungen zum Zuordnen von Warteschlangen zu einem Routingprofil in einer Amazon-Connect-Instance	Schreiben	queue*		
			routing-profile*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} connect:InstanceId	
Associate SecurityKey	Gewährt Berechtigungen zum Zuordnen eines Sicherheitsschlüssels für eine bestehende Amazon-Connect-Instance	Schreiben	instance*		
				connect:InstanceId	
Associate TrafficDistributionGroupUser	Gewährt die Berechtigung zum Zuordnen eines Benutzers zu einer Datenverkehrsverteilungsgruppe in der angegebenen Amazon-Connect-Instance	Schreiben	instance*		connect:DescribeUser connect:SearchUsers
			traffic-distribution-group*		
			user*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				connect:InstanceId aws:ResourceTag/${TagKey} connect:SearchTag/${TagKey}	
AssociateUserProficiencies	Gewährt die Berechtigung zum Zuordnen von Benutzerkompetenzen zu einem Benutzer in einer Amazon-Connect-Instance	Schreiben	instance*		
			user*		
				connect:InstanceId	
BatchAssociateAnalyticsDataSet [nur Berechtigung]	Erteilt die Erlaubnis, Zugriff zu gewähren und die Datensätze mit den angegebenen Daten zu verknüpfen AWS-Konto	Schreiben	instance*		
				connect:InstanceId	
BatchDisassociateAnalyticsDataSet [nur Berechtigung]	Erteilt die Berechtigung, den Zugriff zu widerrufen und die Zuordnung der Datensätze zu den angegebenen Datensätzen aufzuheben AWS-Konto	Schreiben	instance*		
				connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetAttachedFileMetadata	Erteilt die Erlaubnis, Metadaten für mehrere angehängte Dateien von einer Amazon Connect Connect-Instance abzurufen	Lesen	attached-file*		
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
BatchGetFlowAssociation	Gewährt Berechtigungen zum Abrufen von zusammenfassenden Informationen über die Flow-Verknüpfungen für die angegebene Amazon-Connect-Instance	Auflisten	instance*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
BatchPutContact	Gewährt die Berechtigung zum Anlegen von Kontakten in einer Amazon-Connect-Instance	Schreiben	instance*		
			queue		
				connect:InstanceId	
ClaimPhoneNumber	Gewährt die Berechtigung zum Beanspruchen von Telefonnummer-Ressourcen in einer Amazon-Connect-Instance oder Datenverkehr-Verteilungsgruppe	Schreiben	instance*		
			traffic-distribution-group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			wildcard-phone-number*		
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CompleteAttachedFileUpload	Erteilt die Erlaubnis, einen angehängten Datei-Upload in einer Amazon Connect Connect-Instance abzuschließen	Schreiben	attached-file*		
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateAgentStatus	Gewährt Berechtigungen zum Aktualisieren des Agentenstatus in einer Amazon-Connect-Instance	Schreiben	agent-status*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateContactFlow	Gewährt Berechtigungen zum Erstellen eines Gesprächsablaufs in einer Amazon-Connect-Instance	Schreiben	contact-flow*		
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateContactFlowModule	Gewährt Berechtigungen zum Erstellen eines Gesprächsablauf-Moduls in einer Amazon-Connect-Instance	Schreiben	contact-flow-module*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateEvaluationForm	Gewährt die Berechtigung zum Erstellen eines Evaluierungsformulars in der angegebenen Amazon-Connect-Instance. Das Formular kann verwendet werden, um Fragen zur Leistung von Agenten zu definieren und Abschnitte zur Organisation solcher Fragen zu erstellen. Die Bezeichnungen der Fragen und Abschnitte im Evaluierungsformular müssen eindeutig sein	Schreiben	evaluation-form*		
				connect:InstanceId	
CreateHoursOfOperation	Gewährt Berechtigungen zur Erstellung von Betriebsstunden in einer Amazon Connect Instance	Schreiben	hours-of-operation*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateInstance	Gewährt Berechtigungen zum Erstellen einer neuen Amazon-Connect-Instance	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	ds:AuthorizeApplication ds:CheckAlias ds:CreateAlias ds:CreateDirectory ds:CreateIdentityPoolDirectory ds:DeleteDirectory ds:DescribeDirectories ds:UnauthorizeApplication iam:AttachRolePolicy

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					iam:CreateServiceLinkedRole iam:PutRolePolicy

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateIntegrationAssociation	Gewährt Berechtigungen zum Erstellen einer Integrations-Zuordnung mit einer Amazon-Connect-Instance	Schreiben	instance*		app-integrations:CreateApplicationAssociation app-integrations:CreateEventIntegrationAssociation app-integrations:GetApplication cases:GetDomain connect:DescribeInstance ds:DescribeDirectories events:PutRule events:PutTargets

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy mobiletargeting:GetApp voiceid:DescribeDomain wisdom:GetAssistant wisdom:GetKnowledgeBase wisdom:TagResource
			integration-association*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				connect:InstanceId aws:RequestTag/${TagKey} aws:TagKeys	
CreateParticipant	Gewährt die Berechtigung zum Hinzufügen eines Teilnehmers zu einem laufenden Kontakt	Schreiben	contact*		
			instance*		
				connect:InstanceId	
CreatePersistentContactAssociation	Gewährt die Berechtigung zum Erstellen persistenter Kontaktzuordnungen für einen Kontakt	Schreiben	contact*		
			instance*		
				connect:InstanceId	
CreatePredefinedAttribute	Gewährt die Berechtigung zum Erstellen eines vordefinierten Attributs in einer Amazon-Connect-Instance	Schreiben	instance*		
				connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreatePrompt	Gewährt die Berechtigung zum Erstellen einer Aufforderung in einer Amazon-Connect-Instance	Schreiben	prompt*		kms:Decrypt s3:GetObject s3:GetObjectAcl
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateQueue	Gewährt Berechtigungen zum Erstellen einer Warteschlange in einer Amazon-Connect-Instance	Schreiben	hours-of-operation*		
			queue*		
			contact-flow		
			phone-number		
			quick-connect		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateQuickConnect	Gewährt die Berechtigung zum Erstellen einer Schnellverbindung in einer Amazon-Connect-Instance	Write	quick-connect*		
			contact-flow		
			queue		
			user		
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateRoutingProfile	Gewährt die Berechtigung zum Erstellen eines Routingprofils in einer Amazon-Connect-Instance.	Schreiben	queue*		
			routing-profile*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateRule	Gewährt die Berechtigung zum Erstellen einer Regel in einer Amazon-Connect-Instance	Schreiben	rule*		
				connect:InstanceId	
CreateSecurityProfile	Gewährt die Berechtigung zum Erstellen eines Sicherheitsprofils für die angegebene Amazon-Connect-Instance	Schreiben	security-profile*		
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateTaskTemplate	Gewährt die Berechtigung zum Erstellen einer Aufgabenvorlage in einer Amazon-Connect-Instance	Schreiben	task-template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTrafficDistributionGroup	Gewährt die Berechtigung zum Erstellen einer Datenverkehr-Verteilungsgruppe	Schreiben	instance*		
			traffic-distribution-group*		
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateUseCase	Gewährt Berechtigungen zum Erstellen eines Anwendungsfalls für eine Integrations-Zuordnung	Schreiben	instance*		connect:DescribeInstance ds:DescribeDirectories
			integration-association*		
			use-case*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				connect:InstanceId aws:RequestTag/${TagKey} aws:TagKeys	
CreateUser	Gewährt die Berechtigung, einen Benutzer für die angegebene Amazon-Connect-Instance zu erstellen.	Schreiben	routing-profile*		
			security-profile*		
			user*		
			hierarchy-group		
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateUserHierarchyGroup	Gewährt Berechtigungen zum Erstellen einer Benutzerhierarchiegruppe in einer Amazon-Connect-Instance	Schreiben	hierarchy-group		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateView	Gewährt die Berechtigung zum Erstellen einer Ansicht in einer Amazon-Connect-Instance	Schreiben	customer-managed-view*		
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateViewVersion	Gewährt die Berechtigung zum Erstellen einer Ansichtsversion in einer Amazon-Connect-Instance	Schreiben	customer-managed-view*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateVocabulary	Gewährt die Berechtigung zum Erstellen eines Vokabulars in einer Amazon Connect-Instance	Schreiben	vocabulary*		
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
DeactivateEvaluationForm	Gewährt die Berechtigung zum Deaktivieren eines Evaluierungsformulars in der angegebenen Amazon-Connect-Instance. Ein deaktiviertes Formular kann von Benutzern nicht mehr verwendet werden, um neue Evaluierungen zu starten	Schreiben	evaluation-form*		
				connect:InstanceId	
DeleteAttachedFile	Erteilt die Erlaubnis, eine angehängte Datei aus einer Amazon Connect Connect-Instance zu löschen	Schreiben	attached-file*		cases:DeleteRelatedItem

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
DeleteContactEvaluation	Gewährt die Berechtigung zum Löschen einer Kontaktevaluierung in der angegebenen Amazon-Connect-Instance.	Schreiben	contact-evaluation*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteContactFlow	Gewährt Berechtigungen zum Erstellen eines Gesprächsablaufs in einer Amazon-Connect-Instance	Schreiben	contact-flow*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteContactFlowModule	Gewährt Berechtigungen zum Löschen eines Gesprächsablaufs in einer Amazon-Connect-Instance	Schreiben	contact-flow-module*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteEvaluationForm	Gewährt die Berechtigung zum Löschen eines Evaluierungsformulars in der angegebenen Amazon-Connect-Instance. Wenn die Eigenschaft „Version“ angegeben wird, wird nur die angegebene Version des Evaluierungsformulars gelöscht.	Schreiben	evaluation-form*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteHoursOfOperation	Gewährt Berechtigungen zur Löschung von Betriebsstunden in einer Amazon Connect Instance	Schreiben	hours-of-operation*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteInstance	Gewährt Berechtigungen zum Löschen einer Amazon-Connect-Instance. Wenn Sie eine Instance entfernen, wird auch der Link zu einem vorhandenen AWS Verzeichnis entfernt	Schreiben	instance*		ds:DeleteDirectory ds:DescribeDirectories ds:UnauthorizeApplication
				connect:InstanceId aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteIntegrationAssociation	Gewährt Berechtigungen zum Löschen einer Integrations-Zuordnung aus einer Amazon-Connect-Instance. Es dürfen der Zuordnung keine Anwendungsfälle zugeordnet sein	Schreiben	instance*		app-integrations:DeleteApplicationAssociation app-integrations:DeleteEventIntegrationAssociation connect:DescribeInstance ds:DescribeDirectories events:DeleteRule events:ListTargetsByRule events:RemoveTargets

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			integration-association*		
				connect:InstanceId	
DeletePredefinedAttribute	Gewährt die Berechtigung zum Löschen eines vordefinierten Attributs in einer Amazon-Connect-Instance	Schreiben	instance*		
				connect:InstanceId	
DeletePrompt	Gewährt die Berechtigung zum Löschen einer Aufforderung in einer Amazon-Connect-Instance	Schreiben	prompt*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteQueue	Gewährt die Berechtigung zum Löschen einer Warteschlange in einer Amazon-Connect-Instance	Schreiben	queue*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteQuickConnect	Gewährt die Berechtigung zum Löschen einer Schnellverbindung in einer Amazon-Connect-Instance	Schreiben	quick-connect*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteRoutingProfile	Gewährt die Berechtigung zum Löschen von Routingprofilen in einer Amazon-Connect-Instance	Schreiben	routing-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteRule	Gewährt die Berechtigung zum Löschen einer Regel in einer Amazon-Connect-Instance	Schreiben	rule*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteSecurityProfile	Gewährt die Berechtigung zum Löschen eines Sicherheitsprofils in einer Amazon-Connect-Instance	Schreiben	security-profile*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteTaskTemplate	Gewährt die Berechtigung zum Löschen einer Aufgabenvorlage in einer Amazon-Connect-Instance	Schreiben	task-template*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteTrafficDistributionGroup	Gewährt die Berechtigung zum Löschen einer Datenverkehr-Verteilungsgruppe	Schreiben	traffic-distribution-group*		
				aws:ResourceTag/${TagKey}	
DeleteUseCase	Gewährt Berechtigungen zum Löschen eines Anwendungsfalls aus einer Integrations-Zuordnung	Schreiben	instance*		connect:DescribeInstance ds:DescribeDirectories

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			use-case*		
				connect:InstanceId	
DeleteUser	Gewährt die Berechtigung zum Löschen eines Benutzers in einer Amazon-Connect-Instance	Schreiben	user*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteUserHierarchyGroup	Gewährt die Berechtigung zum Löschen einer Benutzerhierarchiegruppe in einer Amazon-Connect-Instance	Schreiben	hierarchy-group*		
				connect:InstanceId	
DeleteView	Gewährt die Berechtigung zum Löschen einer Ansicht in einer Amazon-Connect-Instance	Schreiben	customer-managed-view*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteViewVersion	Gewährt die Berechtigung zum Löschen einer Ansicht in einer Amazon-Connect-Instance	Schreiben	customer-managed-view-version*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteVocabulary	Gewährt Berechtigungen zum Löschen eines Vokabulars in einer Amazon Connect-Instance.	Schreiben	vocabulary*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeAgentStatus	Gewährt Berechtigungen zum Beschreiben eines Agentenstatus in einer Amazon Connect-Instance.	Lesen	agent-status*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeContact	Gewährt die Berechtigung zum Beschreiben eines Kontakts in einer Amazon-Connect-Instance	Lesen	contact*		
				connect:InstanceId	
DescribeContactEvaluation	Gewährt die Berechtigung zum Beschreiben einer Kontaktevaluierung in der angegebenen Amazon-Connect-Instance.	Lesen	contact-evaluation*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeContactFlow	Gewährt die Berechtigung zum Beschreiben eines Gesprächsablaufs in einer Amazon-Connect-Instance	Lesen	contact-flow*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeContactFlowModule	Gewährt die Berechtigung zum Beschreiben eines Gesprächsablauf-Moduls in einer Amazon-Connect-Instance	Lesen	contact-flow-module*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeEvaluationForm	Gewährt die Berechtigung zum Beschreiben eines Evaluierungsformulars in der angegebenen Amazon-Connect-Instance. Wenn die Eigenschaft „Version“ nicht angegeben wird, wird die neueste Version des Evaluierungsformulars beschrieben	Lesen	evaluation-form*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeForecastingPlanningSchedulingIntegration [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben des Status der Prognose- und Planungs-Integration auf einer Amazon-Connect-Instance	Lesen	instance*		
				connect:InstanceId	
DescribeHoursOfOperation	Gewährt die Berechtigung zum Beschreiben von Betriebsstunden in einer Amazon-Connect-Instance	Lesen	hours-of-operation*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeInstance	Gewährt die Berechtigung zum Anzeigen der Details einer Amazon-Connect-Instance und ist auch zum Erstellen einer Instance erforderlich	Lesen	instance*		ds:DescribeDirectories
				connect:InstanceId aws:ResourceTag/${TagKey}	
DescribeInstanceAttribute	Gewährt die Berechtigung zum Anzeigen der Attributdetails einer vorhandenen Amazon-Connect-Instance	Lesen	instance*		
				connect:AttributeType connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeInstanceStorageConfig	Gewährt die Berechtigung zum Anzeigen der Instance-Speicherkonfiguration für eine vorhandene Amazon-Connect-Instance	Lesen	instance*		
				connect:StorageResourceType connect:InstanceId	
DescribePhoneNumber	Gewährt die Berechtigung zum Beschreiben von Telefonnummer-Ressourcen in einer Amazon-Connect-Instance oder Datenverkehr-Verteilungsgruppe	Lesen	phone-number*		
				aws:ResourceTag/${TagKey}	
DescribePredefinedAttribute	Gewährt die Berechtigung zum Beschreiben eines vordefinierten Attributs in einer Amazon-Connect-Instance	Lesen	instance*		
				connect:InstanceId	
DescribePrompt	Gewährt die Berechtigung zum Beschreiben einer Aufforderung in einer Amazon-Connect-Instance	Lesen	prompt*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeQueue	Gewährt die Berechtigung zum Beschreiben einer Warteschlange in einer Amazon-Connect-Instance	Lesen	queue*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeQuickConnect	Gewährt die Berechtigung zum Beschreiben einer Schnellverbindung in einer Amazon-Connect-Instance	Lesen	quick-connect*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeRoutingProfile	Gewährt die Berechtigung zum Beschreiben eines Routingprofils in einer Amazon-Connect-Instance		routing-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeRule	Gewährt die Berechtigung zum Beschreiben einer Regel in einer Amazon-Connect-Instance	Lesen	rule*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeSecurityProfile	Gewährt die Berechtigung zum Beschreiben eines Sicherheitsprofils in einer Amazon-Connect-Instance	Lesen	security-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeTrafficDistributionGroup	Gewährt die Berechtigung zum Beschreiben einer Datenverkehr-Verteilungsgruppe	Lesen	traffic-distribution-group*		
				aws:ResourceTag/${TagKey}	
DescribeUser	Gewährt die Berechtigung zum Beschreiben eines Benutzers in einer Amazon-Connect-Instance	Lesen	user*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeUserHierarchyGroup	Gewährt die Berechtigung zum Beschreiben einer Hierarchiegruppe für eine Amazon-Connect-Instance	Lesen	hierarchy-group*		
				connect:InstanceId	
DescribeUserHierarchyStructure	Gewährt die Berechtigung zum Beschreiben der Hierarchiestruktur für eine Amazon-Connect-Instance	Lesen	instance*		
				connect:InstanceId	
DescribeView	Gewährt die Berechtigung zum Beschreiben einer Ansicht in einer Amazon-Connect-Instance	Lesen	aws-managed-view*		
			customer-managed-view*		
			qualified-aws-managed-view*		
			qualified-customer-managed-view*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeVocabulary	Gewährt die Berechtigung zum Beschreiben eines Vokabulars in einer Amazon Connect-Instance	Lesen	vocabulary*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DisassociateApprovedOrigin	Gewährt die Berechtigung zum Trennen der Zuordnung des genehmigten Ursprungs für eine vorhandene Amazon-Connect-Instance	Schreiben	instance*		
				connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateBot	Gewährt die Berechtigung zum Trennen der Zuordnung eines Lex-Bots für eine vorhandene Amazon-Connect-Instance	Schreiben	instance*		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy lex:DeleteResourcePolicy lex:UpdateResourcePolicy
				connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateCustomerProfilesDomain [nur Berechtigung]	Gewährt die Berechtigung zum Trennen der Zuordnung eines Customer-Profiles-Domain für eine vorhandene Amazon-Connect-Instance	Schreiben	instance*		iam:AttachRolePolicy iam:DeleteRolePolicy iam:DetachRolePolicy iam:GetPolicy iam:GetPolicyVersion iam:GetRolePolicy
DisassociateFlow	Gewährt die Berechtigung zum Trennen einer Ressource von einem Gesprächsablauf in einer Amazon-Connect-Instance	Schreiben	instance*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateInstanceStorageConfig	Gewährt Berechtigungen zum Trennen der Zuordnung des Instance-Speichers für eine vorhandene Amazon-Connect-Instance	Schreiben	instance*		
				connect:StorageResourceType connect:InstanceId	
DisassociateLambdaFunction	Gewährt die Berechtigung zum Trennen der Zuordnung einer Lambda-Funktion für eine vorhandene Amazon-Connect-Instance	Schreiben	instance*		lambda:RemovePermission
				connect:InstanceId	
DisassociateLexBot	Gewährt die Berechtigung zum Trennen der Zuordnung eines Lex-Bots für eine vorhandene Amazon-Connect-Instance	Schreiben	instance*		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy
				connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociatePhoneNumberContactFlow	Gewährt die Berechtigung zum Trennen der Zuordnung von Gesprächsablauf-Ressourcen zu Telefonnummern in einer Amazon-Connect-Instance	Schreiben	phone-number*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DisassociateQueueQuickConnects	Gewährt die Berechtigung zum Trennen der Zuordnung von Schnellverbindungen aus einer Warteschlange in einer Amazon-Connect-Instance	Schreiben	queue*		
			quick-connect*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DisassociateRoutingProfileQueues	Gewährt die Berechtigung zum Trennen der Zuordnung von Warteschlangen aus einem Routingprofil in einer Amazon-Connect-Instance	Schreiben	routing-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateSecurityKey	Gewährt die Berechtigung zum Trennen der Zuordnung des Sicherheitsschlüssels für eine vorhandene Amazon-Connect-Instance	Schreiben	instance*		
				connect:InstanceId	
DisassociateTrafficDistributionGroupUser	Gewährt die Berechtigung, die Zuordnung eines Benutzers zu einer Datenverkehrsverteilungsgruppe in der angegebenen Amazon-Connect-Instance aufzuheben	Schreiben	instance*		
			traffic-distribution-group*		
			user*		
				connect:InstanceId aws:ResourceTag/${TagKey}	
DisassociateUserProficiencies	Gewährt die Berechtigung zum Trennen von Benutzerkompetenzen von einem Benutzer in einer Amazon-Connect-Instance	Schreiben	instance*		
			user*		
				connect:InstanceId	
DismissUserContact	Gewährt die Berechtigung zum Ablehnen eines gekündigten Kontakts von Agent CCP	Schreiben	user*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} connect:InstanceId	
GetAttachedFile	Erteilt die Erlaubnis, eine angehängte Datei von einer Amazon Connect Connect-Instance abzurufen	Lesen	attached-file*		
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
GetContactAttributes	Gewährt die Berechtigung zum Abrufen der Kontaktattribute für den angegebenen Kontakt	Lesen	contact*		
				connect:InstanceId	
GetCurrentMetricData	Gewährt die Berechtigung zum Abrufen aktueller Metrikdaten für Warteschlangen und Routing-Profile in einer Amazon-Connect-Instance	Lesen	queue*		
			routing-profile*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} connect:InstanceId	
GetCurrentUserData	Gewährt die Berechtigung zum Abrufen aktueller Nutzerdaten in einer Amazon-Connect-Instance	Lesen	hierarchy-group*		
			queue*		
			routing-profile*		
			user*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
GetFederationToken	Gewährt die Berechtigung zum Verbund in eine Amazon-Connect-Instance bei Verwendung der SAML-basierten Authentifizierung für das Identitätsmanagement	Lesen	instance*		
				connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetFlowAssociation	Gewährt die Berechtigung zum Abrufen von Informationen über die Flow-Verknüpfungen für die angegebene Amazon-Connect-Instance	Lesen	instance*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
GetMetricData	Gewährt die Berechtigung zum Abrufen historischer Metrikdaten für Warteschlangen in einer Amazon-Connect-Instance	Lesen	queue*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
GetMetricDataV2	Gewährt die Berechtigung zum Abrufen Metrikdaten in einer Amazon-Connect-Instance	Lesen	hierarchy-group*		
			queue*		
			routing-profile*		
			user*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetPromptFile	Gewährt die Berechtigung zum Abrufen von Details über die vordefinierte Amazon-S3-URL einer Aufforderung in einer Amazon-Connect-Instance	Lesen	prompt*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
GetTaskTemplate	Gewährt die Berechtigung, Details zu einer bestimmten Aufgabenvorlage in einer Amazon-Connect-Instance abzurufen		task-template*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
GetTrafficDistribution	Gewährt die Berechtigung zum Lesen der Datenverkehrsverteilung einer Datenverkehr-Verteilungsgruppe	Auflisten	traffic-distribution-group*		
				aws:ResourceTag/${TagKey}	
ImportPhoneNumber	Gewährt die Berechtigung zum Importieren von Telefonnummer-Ressourcen in eine Amazon-Connect-Instance	Schreiben	instance*		sms-voice:DescribePhoneNumbers

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			wildcard-phone-number*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListAgentStatuses	Gewährt die Berechtigung zum Auflisten von Agentenstatus in einer Amazon Connect Instance	Auflisten	wildcard-agent-status*		
ListApprovedOrigins	Gewährt die Berechtigung zum Anzeigen der genehmigten Ursprünge einer vorhandenen Amazon-Connect-Instance	Auflisten	instance*		
				connect:InstanceId	
ListBots	Gewährt die Berechtigung zum Anzeigen der Lex-Bots einer vorhandenen Amazon-Connect-Instance	Auflisten	instance*		
				connect:InstanceId	
ListContactEvaluations	Gewährt die Berechtigung zum Auflisten von Kontaktevaluierungen in der angegebenen Amazon-Connect-Instance.	Auflisten	instance*		
				connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListContactFlowModules	Gewährt die Berechtigung zum Auflisten der Ressourcen von Gesprächsablauf-Modulen in einer Amazon-Connect-Instance	Auflisten	instance*		
ListContactFlows	Gewährt die Berechtigung zum Auflisten von Gesprächsablauf-Ressourcen in einer Amazon-Connect-Instance	Auflisten	wildcard-contact-flow*		
ListContactReferences	Gewährt die Berechtigung zum Auflisten der einem Kontakt zugeordneten Referenzen in einer Amazon-Connect-Instance	Auflisten	contact*		
				connect:InstanceId	
ListDefaultVocabularies	Gewährt Berechtigungen zum Auflisten der einer Amazon Connect-Instance zugeordneten Standardvokabulare	Auflisten	instance*		
				connect:InstanceId	
ListEvaluationFormVersions	Gewährt die Berechtigung zum Auflisten der Versionen eines Evaluierungsformulars in der angegebenen Amazon-Connect-Instance	Auflisten	evaluation-form*		
				connect:InstanceId	
ListEvaluationForms	Gewährt die Berechtigung zum Auflisten von Evaluierungsformularen in der angegebenen Amazon-Connect-Instance	Auflisten	instance*		
				connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListFlowAssociations	Gewährt die Berechtigung zum Auflisten von zusammenfassenden Informationen über die Flow-Verknüpfungen für die angegebene Amazon-Connect-Instance	Auflisten	instance*		
				connect:InstanceId	
ListHoursOfOperations	Gewährt die Berechtigung zum Auflisten von Betriebsstunden-Ressourcen in einer Amazon-Connect-Instance	Auflisten	instance*		
				connect:InstanceId	
ListInstanceAttributes	Gewährt die Berechtigung zum Anzeigen der Attribute einer vorhandenen Amazon-Connect-Instance	Auflisten	instance*		
				connect:InstanceId	
ListInstanceStorageConfigs	Gewährt die Berechtigung zum Anzeigen der Speicherkonfigurationen einer vorhandenen Amazon-Connect-Instance	Auflisten	instance*		
				connect:InstanceId	
ListInstances	Erteilt die Berechtigung zum Anzeigen der Amazon Connect Connect-Instances, die mit einem verknüpft sind AWS-Konto	Auflisten			ds:DescribeDirectories

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListIntegrationAssociations	Gewährt Berechtigungen zum Auflisten von zusammenfassenden Informationen über die Integrations-Zuordnungen für die angegebene Amazon-Connect-Instance	Auflisten	instance*		connect:DescribeInstance ds:DescribeDirectories
				connect:InstanceId	
ListLambdaFunctions	Gewährt die Berechtigung zum Anzeigen der Lambda-Funktionen einer vorhandenen Amazon-Connect-Instance	Auflisten	instance*		
				connect:InstanceId	
ListLexBots	Gewährt die Berechtigung zum Anzeigen der Lex-Bots einer vorhandenen Amazon-Connect-Instance	Auflisten	instance*		
				connect:InstanceId	
ListPhoneNumbers	Gewährt die Berechtigung zum Auflisten von Telefonnummer-Ressourcen in einer Amazon-Connect-Instance	Auflisten	wildcard-legacy-phone-number*		
ListPhoneNumbersV2	Gewährt die Berechtigung zum Auflisten von Telefonnummer-Ressourcen in einer Amazon-Connect-Instance	Auflisten	wildcard-phone-number*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListPredefinedAttributes	Gewährt die Berechtigung zum Auflisten eines vordefinierten Attributs in einer Amazon-Connect-Instance	Auflisten	instance*		
				connect:InstanceId	
ListPrompts	Gewährt die Berechtigung zum Auflisten von Telefonansagen-Ressourcen in einer Amazon-Connect-Instance	Auflisten	instance*		
				connect:InstanceId	
ListQueueQuickConnects	Gewährt die Berechtigung zum Auflisten von Schnellverbindungs-Ressourcen in einer Warteschlange in einer Amazon-Connect-Instance	Auflisten	queue*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
ListQueues	Gewährt die Berechtigung zum Auflisten von Warteschlangen-Ressourcen in einer Amazon-Connect-Instance	Auflisten	wildcard-queue*		
ListQuickConnects	Gewährt die Berechtigung zum Auflisten von Schnellverbindungs-Ressourcen in einer Amazon-Connect-Instance	Auflisten	wildcard-quick-connect*		
ListRealtimeContactAnalysisSegments	Gewährt die Berechtigung zum Auflisten der Analysesegmente für eine Echtzeitanalysesitzung	Lesen	contact*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListRealtimeContactAnalysisSegmentsV2	Gewährt die Berechtigung zum Auflisten der Analysesegmente für eine Echtzeit-Chat-Analysesitzung	Auflisten	contact*		
ListRoutingProfileQueues	Gewährt die Berechtigung zum Auflisten von Warteschlangen-Ressourcen in einem Routingprofil in einer Amazon-Connect-Instance	Auflisten	routing-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
ListRoutingProfiles	Gewährt die Berechtigung zum Auflisten von Routingprofil-Ressourcen in einer Amazon-Connect-Instance	Auflisten	instance*		
				connect:InstanceId	
ListRules	Gewährt Berechtigungen zum Auflisten der einer Amazon Connect-Instance zugeordneten Regeln	Auflisten	instance*		
				connect:InstanceId	
ListSecurityKeys	Gewährt die Berechtigung zum Anzeigen der Sicherheitsschlüssel einer vorhandenen Amazon-Connect-Instance	Auflisten	instance*		
				connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListSecurityProfileApplications	Gewährt die Berechtigung zum Auflisten der einem bestimmten Sicherheitsprofil zugeordneten Anwendungen in einer Amazon-Connect-Instance	Auflisten	security-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
ListSecurityProfilePermissions	Gewährt die Berechtigung zum Auflisten der einem Sicherheitsprofil zugeordneten Berechtigungen in einer Amazon-Connect-Instance	Auflisten	security-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
ListSecurityProfiles	Gewährt die Berechtigung zum Auflisten von Sicherheitsprofil-Ressourcen in einer Amazon-Connect-Instance	Auflisten	instance*		
				connect:InstanceId	
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Amazon-Connect-Ressource	Lesen	agent-status		
			contact-evaluation		
			contact-flow		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			contact-flow-module		
			evaluation-form		
			hierarchy-group		
			hours-of-operation		
			integration-association		
			phone-number		
			prompt		
			queue		
			quick-connect		
			routing-profile		
			rule		
			security-profile		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			traffic-distribution-group		
			use-case		
			user		
			wildcard-phone-number		
				aws:ResourceTag/${TagKey}	
ListTaskTemplates	Gewährt die Berechtigung zum Auflisten von Aufgabenvorlagen-Ressourcen in einer Amazon-Connect-Instance	Auflisten	instance*		
ListTrafficDistributionGroupUsers	Gewährt die Berechtigung zum Auflisten der aktiven Benutzerzuordnungen für eine Datenverkehrsverteilungsgruppe	Auflisten	traffic-distribution-group*		
				aws:ResourceTag/${TagKey}	
ListTrafficDistributionGroups	Gewährt die Berechtigung zum Auflisten von Datenverkehr-Verteilungsgruppen	Auflisten	traffic-distribution-group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListUseCases	Gewährt Berechtigungen zum Auflisten der Anwendungsfälle einer Integrations-Zuordnung	Auflisten	instance*		connect:DescribeInstance ds:DescribeDirectories
				connect:InstanceId	
ListUserHierarchyGroups	Gewährt die Berechtigung zum Auflisten der Hierarchiegruppen-Ressourcen in einer Amazon-Connect-Instance	Auflisten	instance*		
				connect:InstanceId	
ListUserProficiencies	Gewährt die Berechtigung zum Auflisten von Benutzerkompetenzen von einem Benutzer in einer Amazon-Connect-Instance	Auflisten	instance*		
			user*		
				connect:InstanceId	
ListUsers	Gewährt die Berechtigung zum Auflisten von Benutzerressourcen in einer Amazon-Connect-Instance	Auflisten	instance*		
				connect:InstanceId	
ListViewVersions	Gewährt die Berechtigung zum Auflisten von Ansichtsversionen in einer Amazon-Connect-Instance	Auflisten	aws-managed-view*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			customer-managed-view*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
ListViews	Gewährt die Berechtigung zum Auflisten von Ansichten in einer Amazon-Connect-Instance	Auflisten	instance*		
				connect:InstanceId	
MonitorContact	Gewährt die Berechtigung zum Überwachen eines laufenden Kontakts	Schreiben	contact*		
			instance*		
			user*		
				connect:MonitorCapabilities aws:ResourceTag/${TagKey} connect:InstanceId	
PauseContact		Schreiben	contact*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Gewährt die Berechtigung zum Anhalten eines laufenden Kontakts		instance*		
			contact-flow		
				aws:ResourceTag/${TagKey} connect:InstanceId	
PutUserStatus	Gewährt die Berechtigung zum Wechseln des Benutzerstatus in einer Amazon-Connect-Instance.	Schreiben	agent-status*		
			instance*		
			user*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
ReleasePhoneNumber	Gewährt die Berechtigung zur Veröffentlichung von Telefonnummer-Ressourcen in einer Amazon-Connect-Instance	Schreiben	phone-number*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Replicate Instance	Gewährt Berechtigungen zum Erstellen eines Replikats einer Amazon-Connect-Instance	Schreiben	instance*		ds:AuthorizeApplication ds:CheckAlias ds:CreateAlias ds:CreateDirectory ds:CreateIdentityPoolDirectory ds:DeleteDirectory ds:DescribeDirectories ds:UnauthorizeApplication iam:AttachRolePolicy

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					iam:CreateServiceLinkedRole iam:PutRolePolicy
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
ResumeContact	Gewährt die Berechtigung zum Wiederaufnehmen eines angehaltenen Kontakts	Schreiben	contact*		
			instance*		
			contact-flow		
				aws:ResourceTag/${TagKey} connect:InstanceId	
ResumeContactRecording	Gewährt die Berechtigung zum Fortsetzen der Aufzeichnung für den angegebenen Kontakt	Schreiben	contact*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SearchAvailablePhoneNumbers	Gewährt die Berechtigung zum Suchen nach Telefonnummer-Ressourcen in einer Amazon-Connect-Instance oder Datenverkehr-Verteilungsgruppe	Auflisten	wildcard-phone-number*		
SearchContacts	Gewährt die Berechtigung zum Suchen nach Kontakten in einer Amazon-Connect-Instance	Lesen	instance*		connect:DescribeContact
				connect:InstanceId connect:SearchContactsByContactAnalysis	
SearchHoursOfOperations	Gewährt die Berechtigung, Betriebsstunden-Ressourcen in einer Amazon-Connect-Instance zu durchsuchen	Lesen	instance*		connect:DescribeHoursOfOperation
				connect:InstanceId connect:SearchTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SearchPredefinedAttributes	Gewährt die Berechtigung zum Suchen nach vordefinierten Attributen in einer Amazon-Connect-Instance	Lesen	instance*		connect:DescribePredefinedAttribute
				connect:InstanceId	
SearchPrompts	Gewährt die Berechtigung zum Durchsuchen von Aufforderungsressourcen in einer Amazon-Connect-Instance	Lesen	instance*		connect:DescribePrompt
				connect:InstanceId connect:SearchTag/${TagKey}	
SearchQueues	Gewährt die Berechtigung zum Durchsuchen von Warteschlangenressourcen in einer Amazon-Connect-Instance	Lesen	instance*		connect:DescribeQueue
				connect:InstanceId connect:SearchTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SearchQuickConnects	Gewährt die Berechtigung zum Durchsuchen von Schnellverbindungs-Ressourcen in einer Amazon-Connect-Instance	Lesen	instance*		connect:DescribeQuickConnect
				connect:InstanceId connect:SearchTag/${TagKey}	
SearchResourceTags	Erteilt die Berechtigung, nach den verwendeten Tags in einer Amazon-Connect-Instance zu suchen	Auflisten	instance*		
				connect:InstanceId aws:ResourceTag/${TagKey}	
SearchRoutingProfiles	Gewährt die Berechtigung zum Suchen von Routingprofil-Ressourcen in einer Amazon-Connect-Instance	Lesen	instance*		connect:DescribeRoutingProfile
				connect:InstanceId connect:SearchTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SearchSecurityProfiles	Gewährt die Berechtigung zum Suchen nach den Sicherheitsprofil-Ressourcen in einer Amazon-Connect-Instance.	Lesen	instance*		connect:DescribeSecurityProfile
				connect:InstanceId connect:SearchTag/${TagKey}	
SearchUsers	Gewährt die Berechtigung zum Durchsuchen von Benutzerressourcen in einer Amazon-Connect-Instance.	Lesen	instance*		connect:DescribeUser
				connect:InstanceId connect:SearchTag/${TagKey}	
SearchVocabularies	Gewährt die Berechtigung zum Suchen nach Vokabularen in einer Amazon-Connect-Instance.	Auflisten	vocabulary*		
				connect:InstanceId	
SendChatIntegrationEvent	Gewährt die Berechtigung zum Senden von Chat-Integrationsereignissen mithilfe von Amazon Connect API	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartAttachedFileUpload	Erteilt die Erlaubnis, einen angehängten Datei-Upload in einer Amazon Connect Connect-Instance zu starten	Schreiben	attached-file*		cases:CreateRelatedItem
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId connect:UserArn	
StartChatContact	Gewährt die Berechtigung zum Initiieren eines Chats mit der Amazon-Connect-API	Schreiben	contact-flow*		
			contact		
				connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartContactEvaluation	Gewährt die Berechtigung zum Starten einer leeren Evaluierung in der angegebenen Amazon-Connect-Instance auf Basis des Evaluierungsformulars, das für einen bestimmten Kontakt angegeben wurde. Die für die Kontaktevaluierung verwendete Version des Evaluierungsformulars entspricht der aktuell aktivierten Version. Wenn keine Version des Evaluierungsformulars aktiviert ist, kann die Kontaktevaluierung nicht gestartet werden	Schreiben	contact*		
			contact-evaluation*		
			evaluation-form*		
				connect:InstanceId	
StartContactRecording	Gewährt die Berechtigung zum Starten der Aufzeichnung für den angegebenen Kontakt	Schreiben	contact*		
StartContactStreaming	Gewährt die Berechtigung zum Starten von Chat-Streaming mithilfe der Amazon Connect API	Schreiben	instance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartForecastingPlanningSchedulingIntegration [nur Berechtigung]	Gewährt die Berechtigung zum Aktivieren der Prognose- und Planungs-Integration auf einer Amazon-Connect-Instance	Schreiben	instance*		
				connect:InstanceId	
StartOutboundVoiceContact	Gewährt die Berechtigung zum Initiieren ausgehender Anrufe mit der Amazon-Connect-API	Schreiben	contact*		
StartTaskContact	Gewährt die Berechtigung zum Initiieren einer Aufgabe mit der Amazon-Connect-API	Schreiben	contact-flow*		
			contact		
			quick-connect		
			task-template		
				aws:ResourceTag/${TagKey} connect:InstanceId	
StartWebRTCContact	Gewährt die Berechtigung zum Initiieren eines WebRTC-Kontakts mit der Amazon-Connect-API	Schreiben	contact-flow*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				connect:InstanceId	
StopContact	Gewährt die Berechtigung zum Stoppen von Kontakten, die mit der Amazon-Connect-API initiiert wurden. Wenn Sie diese Operation für einen aktiven Kontakt verwenden, endet der Kontakt, auch wenn der Agent ein aktives Telefonat mit einem Kunden führt	Schreiben	contact*		
				connect:InstanceId	
StopContactRecording	Gewährt die Berechtigung zum Beenden der Aufzeichnung für den angegebenen Kontakt	Schreiben	contact*		
StopContactStreaming	Gewährt die Berechtigung zum Stoppen von Chat-Streaming mithilfe der Amazon Connect API	Schreiben	instance*		
StopForecastingPlanningSchedulingIntegration [nur Berechtigung]	Gewährt die Berechtigung zum Deaktivieren der Prognose- und Planungs-Integration auf einer Amazon-Connect-Instance	Schreiben	instance*		
				connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SubmitContactEvaluation	Gewährt die Berechtigung zum Senden einer Kontaktevaluierung in der angegebenen Amazon-Connect-Instance. Die in der Anfrage enthaltenen Antworten werden mit den vorhandenen Antworten in der angegebenen Evaluierung zusammengeführt. Wenn keine Antworten oder Anmerkungen übergeben werden, wird die Evaluierung mit den vorhandenen Antworten und Anmerkungen gesendet. Sie können eine Antwort oder Anmerkung löschen, indem Sie ein leeres Objekt ({}) an die Frage-ID übergeben	Schreiben	contact-evaluation*		
				connect:InstanceId	
SuspendContactRecording	Gewährt die Berechtigung zum Anhalten der Aufzeichnung für den angegebenen Kontakt	Schreiben	contact*		
TagContact	Gewährt die Berechtigung zum Markieren eines Kontakts in einer Amazon-Connect-Instance	Schreiben	contact*		
				connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Markieren einer Amazon-Connect-Ressource	Tagging	agent-status		
			contact-evaluation		
			contact-flow		
			contact-flow-module		
			customer-managed-view		
			evaluation-form		
			hierarchy-group		
			hours-of-operation		
			instance		
			integration-association		
			phone-number		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			prompt		
			queue		
			quick-connect		
			routing-profile		
			rule		
			security-profile		
			task-template		
			traffic-distribution-group		
			use-case		
			user		
			vocabulary		
			wildcard-phone-number		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
TransferContact	Gewährt die Berechtigung zum Übertragen des Kontakts in eine andere Warteschlange oder einen anderen Agent	Schreiben	contact*		
			contact-flow*		
			instance*		
				connect:InstanceId	
UntagContact	Gewährt die Berechtigung zum Aufheben der Markierung eines Kontakts in einer Amazon-Connect-Instance	Schreiben	contact*		
				connect:InstanceId	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Amazon-Connect-Ressource	Tagging	agent-status		
			contact-evaluation		
			contact-flow		
			contact-flow-module		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			customer-managed-view		
			evaluation-form		
			hierarchy-group		
			hours-of-operation		
			instance		
			integration-association		
			phone-number		
			prompt		
			queue		
			quick-connect		
			routing-profile		
			rule		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			security-profile		
			task-template		
			traffic-distribution-group		
			use-case		
			user		
			vocabulary		
			wildcard-phone-number		
				aws:TagKeys	
UpdateAgentStatus	Gewährt Berechtigungen zum Aktualisieren des Agentenstatus in einer Amazon-Connect-Instance	Schreiben	agent-status*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateContact	Gewährt die Berechtigung zum Aktualisieren eines Kontakts in einer Amazon-Connect-Instance	Schreiben	contact*		
				connect:InstanceId	
UpdateContactAttributes	Gewährt die Berechtigung zum Erstellen oder Aktualisieren der Kontaktattribute, die dem angegebenen Kontakt zugeordnet sind	Schreiben	contact*		
				connect:InstanceId	
UpdateContactEvaluation	Gewährt die Berechtigung zum Aktualisieren der Details einer Kontaktevaluierung in der angegebenen Amazon-Connect-Instance. Eine Kontaktevaluierung muss sich im Entwurfsstatus befinden. Die in der Anfrage enthaltenen Antworten werden mit den vorhandenen Antworten in der angegebenen Evaluierung zusammengeführt. Eine Antwort oder Anmerkung kann gelöscht werden, indem ein leeres Objekt ({}) an die Frage-ID übergeben wird	Schreiben	contact-evaluation*		
				connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateContactFlowContent	Gewährt die Berechtigung zum Aktualisieren von Gesprächsablauf-Inhalten in einer Amazon-Connect-Instance	Schreiben	contact-flow*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateContactFlowMetadata	Gewährt die Berechtigung zum Aktualisieren der Metadaten eines Gesprächsablaufs in einer Amazon-Connect-Instance	Schreiben	contact-flow*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateContactFlowModuleContent	Gewährt die Berechtigung zum Aktualisieren von Gesprächsablauf–Modul-Inhalten in einer Amazon-Connect-Instance	Schreiben	contact-flow-module*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateContactFlowModuleMetadata	Gewährt die Berechtigung zum Aktualisieren der Metadaten eines Gesprächsablauf-Moduls in einer Amazon-Connect-Instance	Schreiben	contact-flow-module*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateContactFlowName	Gewährt die Berechtigungen zum Aktualisieren des Namens und der Beschreibung eines Gesprächablaufs in einer Amazon-Connect-Instance	Schreiben	contact-flow*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateContactRoutingData	Gewährt die Berechtigung zum Aktualisieren von Routing-Eigenschaften zu einem Kontakt in einer Amazon-Connect-Instance	Schreiben	contact*		
				connect:InstanceId	
UpdateContactSchedule	Gewährt die Berechtigung zum Aktualisieren des Zeitplans eines Kontakts, der bereits in einer Amazon-Connect-Instance geplant ist	Schreiben	contact*		
				connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateEvaluationForm	Gewährt die Berechtigung zum Aktualisieren der Details einer bestimmten Evaluierungsformularversion in der angegebenen Amazon-Connect-Instance. Die Bezeichnungen der Fragen und Abschnitte im Evaluierungsformular müssen eindeutig sein	Schreiben	evaluation-form*		
				connect:InstanceId	
UpdateHoursOfOperation	Gewährt die Berechtigung zum Aktualisieren von Betriebsstunden in einer Amazon-Connect-Instance		hours-of-operation*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateInstanceAttribute	Gewährt die Berechtigung zum Aktualisieren des Attributs für eine vorhandene Amazon-Connect-Instance	Schreiben	instance*		ds:DescribeDirectories iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy logs:CreateLogGroup
				connect:AttributeType connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateInstanceStorageConfig	Gewährt die Berechtigung zum Aktualisieren der Speicherkonfiguration für eine vorhandene Amazon-Connect-Instance	Schreiben	instance*		ds:DescribeDirectories firehose:DescribeDeliveryStream iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy kinesis:DescribeStream kms:CreateGrant kms:DescribeKey s3:GetBucketAcl

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					s3:GetBucketLocation
				connect:StorageResourceType connect:InstanceId	
UpdateParticipantRoleConfig	Gewährt die Berechtigung zum Aktualisieren von einem Kontakt zugeordneten Teilnehmerrollenkonfigurationen	Schreiben	contact*		
			instance*		
				connect:InstanceId	
UpdatePhoneNumber	Gewährt die Berechtigung zum Aktualisieren von Telefonnummer-Ressourcen in einer Amazon-Connect-Instance oder Datenverkehr-Verteilungsgruppe	Schreiben	instance*		
			phone-number*		
			traffic-distribution-group*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdatePhoneNumberMetadata	Gewährt die Berechtigung zum Aktualisieren der Metadaten einer Telefonnummer-Ressource in einer Amazon-Connect-Instance oder Datenverkehrsverteilungsgruppe	Schreiben	phone-number*		
				aws:ResourceTag/${TagKey}	
UpdatePredefinedAttribute	Gewährt die Berechtigung zum Aktualisieren eines vordefinierten Attributs in einer Amazon-Connect-Instance	Schreiben	instance*		
				connect:InstanceId	
UpdatePrompt	Gewährt die Berechtigung, den Namen, die Beschreibung und den Amazon-S3-URI einer Aufforderung in einer Amazon-Connect-Instance zu aktualisieren	Schreiben	prompt*		kms:Decrypt s3:GetObject s3:GetObjectAcl
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateQueueHoursOfOperation	Gewährt die Berechtigung, Betriebsstunden in eine Warteschlange in einer Amazon-Connect-Instance aufzunehmen	Schreiben	hours-of-operation*		
			queue*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateQueueMaxContacts	Gewährt die Berechtigung zum Aktualisieren der Warteschlangen-Kapazität in einer Amazon-Connect-Instance	Schreiben	queue*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateQueueName	Gewährt die Berechtigung zum Aktualisieren des Namens und der Beschreibung einer Warteschlange in einer Amazon-Connect-Instance	Schreiben	queue*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateQueueOutboundCallerConfig	Gewährt die Berechtigung, die Konfiguration für ausgehende Anrufer in eine Warteschlange in einer Amazon-Connect-Instance aufzunehmen	Schreiben	queue*		
			contact-flow		
			phone-number		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateQueueStatus	Gewährt die Berechtigung zum Aktualisieren des Warteschlangenstatus in einer Amazon-Connect-Instance	Schreiben	queue*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateQuickConnectConfig	Gewährt die Berechtigung zum Aktualisieren der Konfiguration einer Schnellverbindung in einer Amazon-Connect-Instance	Schreiben	quick-connect*		
			contact-flow		
			queue		
			user		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateQuickConnectName	Gewährt die Berechtigung zum Aktualisieren des Namens und der Beschreibung einer Schnellverbindung in einer Amazon-Connect-Instance	Schreiben	quick-connect*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateRoutingProfileAgentAvailabilityTimer	Erteilt die Berechtigung zum Aktualisieren des Routingprofil-Agentenverfügbarkeitstimers in einer Amazon-Connect-Instance	Schreiben	routing-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateRoutingProfileConcurrency	Gewährt die Berechtigung zum Aktualisieren der Parallelität in einem Routingprofil in einer Amazon-Connect-Instance	Schreiben	routing-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateRoutingProfileDefaultOutboundQueue	Gewährt die Berechtigung zum Aktualisieren der ausgehenden Warteschlange in einem Routingprofil in einer Amazon-Connect-Instance	Schreiben	queue*		
			routing-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateRoutingProfileName	Gewährt die Berechtigung zum Aktualisieren des Namens und der Beschreibung eines Routingprofils in einer Amazon-Connect-Instance	Schreiben	routing-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateRoutingProfileQueues	Gewährt die Berechtigung zum Aktualisieren der Warteschlangen im Routingprofil in einer Amazon-Connect-Instance	Schreiben	routing-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateRule	Gewährt die Berechtigung zum Aktualisieren einer Rolle für eine vorhandene Amazon-Connect-Instance	Schreiben	rule*		
				connect:InstanceId	
UpdateSecurityProfile	Gewährt die Berechtigung zum Aktualisieren einer Sicherheitsprofilgruppe für einen Benutzer in einer Amazon-Connect-Instance	Schreiben	security-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateTaskTemplate	Gewährt die Berechtigung zum Aktualisieren der Aufgabenvorlage, die zu einer Amazon-Connect-Instance gehört	Schreiben	task-template*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateTrafficDistribution	Gewährt die Berechtigung zum Aktualisieren der Datenverkehrsverteilung einer Datenverkehr-Verteilungsgruppe	Schreiben	traffic-distribution-group*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateUserHierarchy	Gewährt die Berechtigung zum Aktualisieren einer Hierarchiegruppe für einen Benutzer in einer Amazon-Connect-Instance	Schreiben	user*		
			hierarchy-group		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateUserHierarchyGroupName	Gewährt die Berechtigung zum Aktualisieren des Namens einer Benutzerhierarchiegruppe in einer Amazon-Connect-Instance	Schreiben	hierarchy-group*		
				connect:InstanceId	
UpdateUserHierarchyStructure	Gewährt die Berechtigung zum Aktualisieren der Benutzerhierarchiestruktur in einer Amazon-Connect-Instance	Schreiben	instance*		
				connect:InstanceId	
UpdateUserIdentityInfo	Gewährt die Berechtigung zum Aktualisieren von Identitätsinformationen für einen Benutzer in einer Amazon-Connect-Instance	Schreiben	user*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateUserPhoneConfig	Gewährt die Berechtigung zum Aktualisieren der Telefonkonfigurations-Einstellungen für einen Benutzer in einer Amazon-Connect-Instance	Schreiben	user*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateUserProficiencies	Gewährt die Berechtigung zum Aktualisieren von Benutzerkompetenzen von einem Benutzer in einer Amazon-Connect-Instance	Schreiben	instance*		
			user*		
				connect:InstanceId	
UpdateUserRoutingProfile	Gewährt die Berechtigung zum Aktualisieren eines Routingprofils für einen Benutzer in einer Amazon-Connect-Instance	Schreiben	routing-profile*		
			user*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateUserSecurityProfiles	Gewährt die Berechtigung zum Aktualisieren von Sicherheitsprofilen für einen Benutzer in einer Amazon-Connect-Instance	Schreiben	security-profile*		
			user*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateViewContent	Gewährt die Berechtigung zum Aktualisieren des Inhalts einer Ansicht in einer Amazon-Connect-Instance	Schreiben	customer-managed-view*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateViewMetadata	Gewährt die Berechtigung zum Aktualisieren der Metadaten einer Ansicht in einer Amazon-Connect-Instance	Schreiben	customer-managed-view*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Von Amazon Connect definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der

Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
instance	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}`	aws:ResourceTag/${TagKey}
contact	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/contact/${ContactId}`	
user	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/agent/${UserId}`	aws:ResourceTag/${TagKey}
routing-profile	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/routing-profile/${RoutingProfileId}`	aws:ResourceTag/${TagKey}
security-profile	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/security-profile/${SecurityProfileId}`	aws:ResourceTag/${TagKey}
hierarchy-group	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/agent-group/${HierarchyGroupId}`	aws:ResourceTag/${TagKey}
queue	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/queue/${QueueId}`	aws:ResourceTag/${TagKey}
wildcard-queue	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/queue/*`	

Ressourcentypen	ARN	Bedingungsschlüssel
quick-connect	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/transfer-destination/${QuickConnectId}	aws:ResourceTag/${TagKey}
wildcard-quick-connect	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/transfer-destination/*	
contact-flow	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/contact-flow/${ContactFlowId}	aws:ResourceTag/${TagKey}
task-template	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/task-template/${TaskTemplateId}	aws:ResourceTag/${TagKey}
contact-flow-module	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/flow-module/${ContactFlowModuleId}	aws:ResourceTag/${TagKey}
wildcard-contact-flow	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/contact-flow/*	
hours-of-operation	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/operating-hours/${HoursOfOperationId}	aws:ResourceTag/${TagKey}
agent-status	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/agent-state/${AgentStatusId}	aws:ResourceTag/${TagKey}
wildcard-agent-status	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/agent-state/*	

Ressourcentypen	ARN	Bedingungsschlüssel
legacy-phone-number	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/phone-number/${PhoneNumberId}	
wildcard-legacy-phone-number	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/phone-number/*	
phone-number	arn:${Partition}:connect:${Region}:${Account}:phone-number/${PhoneNumberId}	aws:ResourceTag/${TagKey}
wildcard-phone-number	arn:${Partition}:connect:${Region}:${Account}:phone-number/*	aws:ResourceTag/${TagKey}
integration-association	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/integration-association/${IntegrationAssociationId}	aws:ResourceTag/${TagKey}
use-case	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/use-case/${UseCaseId}	aws:ResourceTag/${TagKey}
vocabulary	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/vocabulary/${VocabularyId}	aws:ResourceTag/${TagKey}
traffic-distribution-group	arn:${Partition}:connect:${Region}:${Account}:traffic-distribution-group/${TrafficDistributionGroupId}	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
rule	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/rule/${RuleId}	aws:ResourceTag/${TagKey}
evaluation-form	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/evaluation-form/${FormId}	aws:ResourceTag/${TagKey}
contact-evaluation	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/contact-evaluation/${EvaluationId}	aws:ResourceTag/${TagKey}
prompt	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/prompt/${PromptId}	aws:ResourceTag/${TagKey}
customer-managed-view	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/view/${ViewId}	aws:ResourceTag/${TagKey}
aws-managed-view	arn:${Partition}:connect:${Region}:aws:view/${ViewId}	
qualified-customer-managed-view	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/view/${ViewId}:${ViewQualifier}	aws:ResourceTag/${TagKey}
qualified-aws-managed-view	arn:${Partition}:connect:${Region}:aws:view/${ViewId}:${ViewQualifier}	
customer-managed-view-version	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/view/${ViewId}:${ViewVersion}	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
attached-file	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/file/${FileId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Connect

Amazon Connect definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff mithilfe von Tag-Schlüssel-Wert-Paaren in der Anforderung	String
aws:ResourceTag/${TagKey}	Filtert Aktionen mithilfe von Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert den Zugriff mithilfe von Tag-Schlüsseln in der Anforderung	ArrayOfString
connect:AttributeType	Filtert den Zugriff nach dem Attributtyp der Amazon Connect Instance	Zeichenfolge
connect:InstanceId	Filtert den Zugriff, indem Verbund auf angegebene Amazon-Connect-Instances beschränkt wird	String
connect:MonitorCapabilities	Filtert den Zugriff, indem die Überwachungsfunktionen des Benutzers in der Anfrage eingeschränkt werden	ArrayOfString

Bedingungsschlüssel	Beschreibung	Typ
connect:SearchContactsByContactAnalysis	Filtert den Zugriff, indem Suchanfragen anhand von Analyseausgaben von Amazon Connect Contact Lens eingeschränkt werden	ArrayOfString
connect:SearchTag/${TagKey}	Filtert den Zugriff nach der TagFilter Bedingung, die in der Suchanfrage erfüllt wurde	String
connect:StorageResourceType	Filtert den Zugriff, indem der Speicherressourcentyp der Instance-Speicherkonfiguration von Amazon Connect beschränkt wird	String
connect:UserArn	Filtert den Zugriff nach UserArn	ARN

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Connect Cases

Amazon Connect Cases (Servicepräfix: `cases`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Connect Cases definierte Aktionen
- Von Amazon Connect Cases definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Connect Cases

Von Amazon Connect Cases definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetField	Gewährt die Berechtigung zum Abrufen von Informationen zu den Feldern in der Fall-Domain	Lesen	Domain*		
			Field*		
BatchPutFieldOptions	Gewährt die Berechtigung zum Aktualisieren der Feldoptionen in der Fall-Domain	Schreiben	Domain*		
			Field*		
CreateCase	Gewährt die Berechtigung zum Erstellen eines Falls in der Fall-Domain	Schreiben	Case*		
			Domain*		
			Field*		
			Template*		
				connect:UserArn	
CreateDomain	Gewährt die Berechtigung zum Erstellen einer neuen Fall-Domain	Schreiben			
CreateField	Gewährt die Berechtigung zum Erstellen eines Feldes in der Fall-Domain	Schreiben	Domain*		
			Field*		
CreateLayout	Gewährt die Berechtigung zum Erstellen eines Layouts in der Fall-Domain	Schreiben	Domain*		
			Layout*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateRelatedItem	Gewährt die Berechtigung zum Erstellen eines verwandten Elements, das einem Fall in der Fall-Domain zugeordnet ist	Schreiben	Case*		
			Domain*		
			RelatedItem*		
				connect:UserArn	
CreateTemplate	Gewährt die Berechtigung zum Erstellen einer Vorlage in der Fall-Domain	Schreiben	Domain*		
			Layout*		
			Template*		
DeleteDomain	Gewährt die Berechtigung zum Löschen der Domain	Schreiben	Domain*		
DeleteField	Erteilt die Erlaubnis, das Feld in der Falldomäne zu löschen	Schreiben	Domain*		
			Field*		
DeleteLayout	Erteilt die Berechtigung zum Löschen des Layouts in der Kundenvorgangsdomäne	Schreiben	Domain*		
			Layout*		
DeleteRelatedItem [nur Berechtigung]	Erteilt die Berechtigung zum Löschen eines verwandten Elements, das einem Kundenvorgang in der Kundenvorgangsdomäne zugeordnet ist	Schreiben	Case*		
			Domain*		
			RelatedItem*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteTemplate	Erteilt die Berechtigung zum Löschen der Vorlage in der Kundenvorgangsdomäne	Schreiben	Domain*		
			Template*		
GetCase	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Fall in der Fall-Domain	Lesen	Case*		
			Domain*		
			Field*		
GetCaseAuditEvents	Erteilt die Berechtigung, den Auditverlauf eines Falls einzusehen	Lesen	Case*		
			Domain*		
GetCaseEventConfiguration	Gewährt die Berechtigung zum Abrufen von Informationen zur Konfiguration von Fallereignissen in der Fall-Domain	Lesen	Domain*		
GetDomain	Gewährt die Berechtigung zum Abrufen von Informationen über die Fall-Domain	Lesen	Domain*		
GetLayout	Gewährt die Berechtigung zum Abrufen von Informationen zum Layout in der Fall-Domain	Lesen	Domain*		
			Layout*		
GetTemplate	Gewährt die Berechtigung zum Abrufen von Informationen über die Vorlage in der Fall-Domain	Lesen	Domain*		
			Template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListCasesForContact	Gewährt die Berechtigung zum Auflisten von Fällen für einen bestimmten Kontakt in der Fall-Domain	Auflisten	Domain*		
ListDomains	Erteilt die Berechtigung zum Auflisten aller Domains im AWS-Konto	Auflisten			
ListFieldOptions	Gewährt die Berechtigung zum Auflisten von Feldoptionen für ein einzeln ausgewähltes Feld in der Fall-Domain	Auflisten	Domain* Field*		
ListFields	Gewährt die Berechtigung zum Auflisten von Feldern in der Fall-Domain	Auflisten	Domain*		
ListLayouts	Erteilt die Berechtigung zum Auflisten von Layouts in der Fall-Domain	Auflisten	Domain*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für die angegebene Ressource	Lesen			
ListTemplates	Gewährt die Berechtigung zum Auflisten von Vorlagen in der Fall-Domain	Auflisten	Domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutCaseEventConfiguration	Gewährt die Berechtigung zum Einfügen oder Aktualisieren der Fallereigniskonfiguration in der Fall-Domain	Schreiben	Domain*		
SearchCases	Gewährt die Berechtigung zum Suchen nach Fällen in der Fall-Domain	Lesen	Domain*		
SearchRelatedItems	Gewährt die Berechtigung, in der Fall-Domain nach verwandten Elementen zu suchen, die mit dem Fall verknüpft sind	Lesen	Case*		
			Domain*		
TagResource	Gewährt die Berechtigung zum Hinzufügen der angegebenen Tags zur angegebenen Ressource	Tagging	Case		
			Domain		
			Field		
			Layout		
			RelatedItem		
			Template		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UntagResource	Gewährt die Berechtigung zum Entfernen der angegebenen Tags aus der angegebenen Ressource	Tagging	Case		
			Domain		
			Field		
			Layout		
			RelatedItem		
			Template		
				aws:TagKeys	
UpdateCase	Gewährt die Berechtigung zum Aktualisieren der Feldwerte für den Fall in der Fall-Domain	Schreiben	Case*		
			Domain*		
			Field*		
				connect:UserArn	
UpdateField	Gewährt die Berechtigung zum Aktualisieren eines Feldes in der Fall-Domain	Schreiben	Domain*		
			Field*		
UpdateLayout	Gewährt die Berechtigung zum Aktualisieren eines Layouts in der Fall-Domain	Schreiben	Domain*		
			Layout*		
UpdateTemplate		Schreiben	Domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Gewährt die Berechtigung zum Aktualisieren der Vorlage in der Fall-Domain		Template*		

Von Amazon Connect Cases definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Case	`arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/case/${CaseId}`	aws:ResourceTag/${TagKey}
Domain	`arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}`	aws:ResourceTag/${TagKey}
Field	`arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/field/${FieldId}`	aws:ResourceTag/${TagKey}
Layout	`arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/layout/${LayoutId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
RelatedItem	`arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/case/${CaseId}/related-item/${RelatedItemId}`	aws:ResourceTag/${TagKey}
Template	`arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/template/${TemplateId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Connect Cases

Amazon Connect Cases definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch Tags, die in der Anforderung übergeben werden	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf Tags, die der Ressource zugeordnet sind	String
aws:TagKeys	Filtert den Zugriff basierend auf Tag-Schlüsseln, die in der Anforderung übergeben werden	ArrayOfString
connect:UserArn	Filtert den Zugriff nach Verbindungen UserArn	ARN

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Connect Customer Profiles

Amazon Connect Customer Profiles (Servicepräfix: `profile`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Connect Customer Profiles definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie

den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddProfileKey	Gewährt die Berechtigung zum Hinzufügen eines Profilschlüssels	Schreiben	domains*		
CreateCalculatedAttributeDefinition	Gewährt die Berechtigung zum Erstellen einer berechneten Attributdefinition in der Domain	Schreiben	calculated-attributes*	aws:RequestTag/${TagKey} aws:TagKeys	
			domains*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDomain	Gewährt die Berechtigung zum Erstellen einer Domain	Schreiben	domains*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole
CreateEventStream	Gewährt die Berechtigung zum Platzieren eines Event-Streams in einer Domain	Schreiben	domains*		iam:PutRolePolicy kinesis:DescribeStreamSummary
			event-streams*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateIntegrationWorkflow	Gewährt die Berechtigung zum Erstellen eines Integrationsworkflows in einer Domain	Schreiben	domains*		
			integrations*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfile	Gewährt die Berechtigung zum Erstellen eines Profils in der Domain	Schreiben	domains*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteCalculatedAttributeDefinition	Gewährt die Berechtigung zum Löschen einer berechneten Attributdefinition in der Domain	Schreiben	calculated-attributes*		
			domains*		
DeleteDomain	Gewährt die Berechtigung zum Löschen einer Domain	Schreiben	domains*		
DeleteEventStream	Gewährt die Berechtigung zum Löschen eines Event-Streams in einer Domain	Schreiben	domains*		iam:DeleteRolePolicy
			event-streams*		
DeleteIntegration	Gewährt die Berechtigung zum Löschen einer Integration in einer Domain	Write	domains*		
			integrations*		
DeleteProfile	Gewährt die Berechtigung zum Löschen eines Profils	Write	domains*		
DeleteProfileKey	Gewährt die Berechtigung zum Löschen eines Profilschlüssels	Write	domains*		
DeleteProfileObject	Gewährt die Berechtigung zum Löschen eines Profilobjekts	Write	domains*		
			object-types*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteProfileObjectType	Gewährt die Berechtigung zum Löschen eines bestimmten Profilobjekttyps in der Domain	Schreiben	domains*		
			object-types*		
DeleteWorkflow	Gewährt die Berechtigung zum Löschen eines Workflows in einer Domain	Schreiben	domains*		
DetectProfileObjectType	Gewährt die Berechtigung zum automatischen Erkennen eines Objekttyps	Lesen	domains*		
GetAutoMergingPreview	Gewährt die Berechtigung zum Abrufen einer Vorschau des automatischen Zusammenführens in einer Domain	Lesen	domains*		
GetCalculatedAttributeDefinition	Gewährt die Berechtigung zum Erhalten einer berechneten Attributdefinition in der Domain	Lesen	calculated-attributes*		
			domains*		
GetCalculatedAttributeForProfile	Gewährt die Berechtigung zum Abrufen eines berechneten Attributs für ein bestimmtes Profil in der Domain	Lesen	calculated-attributes*		
			domains*		
GetDomain	Gewährt die Berechtigung zum Abrufen einer bestimmten Domain in einem Konto	Lesen	domains*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetEventStream	Gewährt die Berechtigung zum Erhalten eines spezifischen Event-Streams in einer Domain	Lesen	domains*		kinesis:DescribeStreamSummary
			event-streams*		
GetIdentityResolutionJob	Gewährt die Berechtigung zum Abrufen eines Identität sauflösungs-Auftrags in einer Domain	Lesen	domains*		
GetIntegration	Gewährt die Berechtigung zum Abrufen einer bestimmten Integration in einer Domain	Lesen	domains*		
			integrations*		
GetMatches	Gewährt die Berechtigung zum Abrufen von übereinstimmenden Profilen in einer Domain	Auflisten	domains*		
GetProfileObjectType	Gewährt die Berechtigung zum Abrufen eines bestimmten Profilobjekttyps in der Domain	Read	domains*		
			object-types*		
GetProfileObjectTypeTemplate	Gewährt die Berechtigung zum Abrufen einer bestimmten Objekttypvorlage	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetSimilarProfiles	Gewährt die Berechtigung zum Abrufen aller ähnlichen Profile in der Domain	Auflisten	domains*		
GetWorkflow	Gewährt die Berechtigung zum Abrufen von Workflowdetails in einer Domain	Lesen	domains*		
GetWorkflowSteps	Gewährt die Berechtigung zum Abrufen von Workflowschrittdetails in einer Domain	Lesen	domains*		
ListAccountIntegrations	Gewährt die Berechtigung zum Auflisten aller Integrationen im Konto	Auflisten			
ListCalculatedAttributeDefinitions	Gewährt die Berechtigung zum Auflisten aller berechneten Attributdefinition in der Domain	Auflisten	domains*		
ListCalculatedAttributesForProfile	Gewährt die Berechtigung zum Auflisten aller berechneten Attribute für ein bestimmtes Profil in der Domain	Auflisten	domains*		
ListDomains	Gewährt die Berechtigung zum Auflisten aller Domains in einem Konto	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListEventStreams	Gewährt die Berechtigung zum Auflisten aller Event-Streams in einer spezifischen Domain	Auflisten	domains*		
ListIdentityResolutionJobs	Gewährt die Berechtigung zum Auflisten von Identitätsauflösungs-Aufträgen in einer Domain	Auflisten	domains*		
ListIntegrations	Gewährt die Berechtigung zum Auflisten aller Integrationen in einer bestimmten Domain	List	domains*		
ListProfileObjectTypeTemplates	Gewährt die Berechtigung, alle Vorlagen für den Profilobjekttyp im Konto aufzulisten	List			
ListProfileObjectTypes	Gewährt die Berechtigung zum Auflisten aller Profilobjekttypen in der Domain	List	domains*		
ListProfileObjects	Gewährt die Berechtigung zum Auflisten aller Profilobjekte für ein Profil	Auflisten	domains* object-types*		
ListRuleBasedMatches	Gewährt die Berechtigung zum Auflisten aller regelbasierten Übereinstimmungsergebnisse in der Domain	Auflisten	domains*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen	calculated-attributes		
			domains		
			event-streams		
			integrations		
			object-types		
ListWorkflows	Gewährt die Berechtigung zum Auflisten aller Workflows in einer bestimmten Domain	Auflisten	domains*		
MergeProfiles	Gewährt die Berechtigung, Profile in einer Domain zusammenzuführen	Schreiben	domains*		
PutIntegration	Gewährt die Berechtigung zum Ablegen einer Integration in einer Domain	Write	domains*		
			integrations*	aws:RequestTag/${TagKey} aws:TagKeys	
PutProfileObject	Gewährt die Berechtigung zum Ablegen eines Objekts für ein Profil	Write	domains*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			object-types*		
PutProfileObjectType	Gewährt die Berechtigung zum Ablegen eines bestimmten Profilobjekttyps in der Domain	Write	domains*		
			object-types*	aws:RequestTag/${TagKey} aws:TagKeys	
SearchProfiles	Gewährt die Berechtigung zum Suchen nach Profilen in einer Domain	Read	domains*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Ressource	Markieren	calculated-attributes		
			domains		
			event-streams		
			integrations		
			object-types		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Ressource	Tagging	calculated-attributes		
			domains		
			event-streams		
			integrations		
			object-types		
				aws:TagKeys	
UpdateCalculatedAttributeDefinition	Gewährt die Berechtigung zum Aktualisieren einer berechneten Attributdefinition in der Domain	Schreiben	calculated-attributes*		
			domains*		
UpdateDomain	Gewährt die Berechtigung zum Aktualisieren einer Domain	Write	domains*		iam:CreateServiceLinkedRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateProfile	Gewährt die Berechtigung zum Aktualisieren eines Profils in der Domain	Write	domains*		

Von Amazon Connect Customer Profiles definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
domains	`arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}`	aws:ResourceTag/${TagKey}
object-types	`arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/object-types/${ObjectTypeName}`	aws:ResourceTag/${TagKey}
integrations	`arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/integrations/${Uri}`	aws:ResourceTag/${TagKey}
event-streams	`arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/event-streams/${EventStreamName}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
calculated-attributes	`arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/calculated-attributes/${CalculatedAttributeName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Connect Customer Profiles

Amazon Connect Customer Profiles definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff entsprechend eines Schlüssels, der in der Anforderung vorhanden ist, die der Benutzer an den EKS-Service sendet	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff anhand eines Tag-Schlüssel-Wert-Paares	String
aws:TagKeys	Filtert den Zugriff nach der Liste aller Tag-Schlüsselnamen, die in der Anforderung vorhanden sind, die der Benutzer an den EKS-Service sendet	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Connect Voice ID

Amazon Connect Voice ID (Service-Präfix: `voiceid`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Connect Voice ID definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateFraudster	Gewährt die Berechtigung zum Zuordnen eines Fraudster zu einer Watchlist	Schreiben	domain*		
CreateDomain	Gewährt die Berechtigung zum Erstellen einer Domain	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWatchlist	Gewährt die Berechtigung zum Erstellen einer Watchlist	Schreiben	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteDomain	Gewährt die Berechtigung zum Löschen einer Domain	Schreiben	domain*		
DeleteFraudster	Gewährt die Berechtigung zum Löschen eines Fraudster	Schreiben	domain*		
DeleteSpeaker	Gewährt die Berechtigung zum Löschen eines Speaker	Schreiben	domain*		
DeleteWatchlist	Gewährt die Berechtigung zum Löschen einer Watchlist	Schreiben	domain*		
DescribeComplianceConsent [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben der Compliance-Zustimmung	Lesen			
DescribeDomain	Gewährt die Berechtigung zum Beschreiben einer Domain	Lesen	domain*		
DescribeFraudster	Gewährt die Berechtigung zum Beschreiben eines Fraudster	Lesen	domain*		
DescribeFraudsterRegistrationJob	Gewährt die Berechtigung zum Beschreiben eines Fraudster Registration Jobs	Lesen	domain*		
DescribeSpeaker	Gewährt die Berechtigung zum Beschreiben eines Speaker	Lesen	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeSpeakerEnrollmentJob	Gewährt die Berechtigung zum Beschreiben eines Speaker Enrollment Jobs	Lesen	domain*		
DescribeWatchlist	Gewährt die Berechtigung zum Beschreiben einer Watchlist	Lesen	domain*		
DisassociateFraudster	Gewährt die Berechtigung zum Aufheben der Zuordnung eines Fraudster zu einer Watchlist	Schreiben	domain*		
EvaluateSession	Gewährt die Berechtigung zum Auswerten einer Sitzung	Schreiben	domain*		
ListDomains	Gewährt die Berechtigung zum Auflisten der Domains für ein Konto	Auflisten			
ListFraudsterRegistrationJobs	Gewährt die Berechtigung zum Auflisten von Fraudster Registration Jobs für eine Domain	Auflisten	domain*		
ListFraudsters	Gewährt die Berechtigung zum Auflisten von Fraudsters für eine Domain oder Watchlist	Auflisten	domain*		
ListSpeakerEnrollmentJobs	Gewährt die Berechtigung zum Auflisten von Speaker Enrollment Jobs für eine Domain	Auflisten	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListSpeakers	Gewährt die Berechtigung zum Auflisten von Speakers für eine Domain	Auflisten	domain*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Voice ID-Ressource	Lesen	domain		
ListWatchlists	Gewährt die Berechtigung zum Auflisten von Watchlists für eine Domain	Auflisten	domain*		
OptOutSpeaker	Gewährt die Berechtigung zum Abmelden eines Speaker	Schreiben	domain*		
RegisterComplianceConsent [nur Berechtigung]	Gewährt die Berechtigung zum Registrieren der Compliance-Zustimmung	Schreiben			
StartFraudsterRegistrationJob	Gewährt die Berechtigung zum Starten eines Fraudster Registration Jobs	Schreiben	domain*		
StartSpeakerEnrollmentJob	Gewährt die Berechtigung zum Starten eines Speaker Enrollment Jobs	Schreiben	domain*		
TagResource	Gewährt die Berechtigung zum Markieren einer Voice ID-Ressource	Markierung	domain		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen eines Tags von einer Voice ID-Ressource	Markierung	domain		
				aws:TagKeys	
UpdateDomain	Gewährt die Berechtigung zum Aktualisieren einer Domain	Schreiben	domain*		
UpdateWatchlist	Gewährt die Berechtigung zum Aktualisieren einer Watchlist	Schreiben	domain*		

Von Amazon Connect Voice ID definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
domain	`arn:${Partition}:voiceid:${Region}:${Account}:domain/${DomainId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Connect Voice ID

Amazon Connect Voice ID definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch Tags, die in der Anforderung übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf Tags, die der Ressource zugeordnet sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf Tag-Schlüsseln, die in der Anforderung übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Connector Service

AWS Connector Service (Service-Präfix: `awsconnector`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Vom AWS Connector Service definierte Aktionen
- Vom AWS Connector Service definierte Ressourcentypen
- Bedingungsschlüssel für AWS Connector Service

Vom AWS Connector Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetConnectorHealth [nur Berechtigung]	Ruft alle Zustandsmetriken ab, die vom Server Migration Connector veröffentlicht wurden.	Read			
RegisterConnector [nur Berechtigung]	Registriert AWS Connector beim AWS Connector Service.	Write			
ValidateConnectorId [nur Berechtigung]	Validiert die Server Migration Connector-ID, die beim AWS Connector Service registriert wurde.	Read			

Vom AWS Connector Service definierte Ressourcentypen

AWS Connector Service unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf AWS Connector Service zu erlauben, geben Sie in Ihrer Richtlinie `"Resource": "*"` an.

Bedingungsschlüssel für AWS Connector Service

Connector Service umfasst keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Management Console Mobile App

AWS Management Console Mobile App (Servicepräfix: `consoleapp`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungsschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Management Console Mobile App definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn

die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDeviceIdentity	Gewährt die Berechtigung zum Abrufen der Geräte-ID für ein Gerät der Console Mobile App	Lesen	DeviceIdentity*		
ListDeviceIdentities	Gewährt die Berechtigung zum Abrufen einer Liste von Geräte-IDs	Auflisten			

Von AWS Management Console Mobile App definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
DeviceIdentity	`arn:${Partition}:consoleapp::${Account}:device/${DeviceId}/identity/${IdentityId}`	

Bedingungsschlüssel für AWS Management Console Mobile App

Die mobile App „Console“ hat keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Consolidated Billing

AWS Consolidated Billing (Servicepräfix: `consolidatedbilling`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Consolidated Billing definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAccountBillingRole [nur Berechtigung]	Gewährt die Berechtigung zum Erhalten der Kontorolle (Zahler, Verknüpft, Regulär)	Lesen			
ListLinkedAccounts [nur Berechtigung]	Gewährt die Berechtigung zum Erhalten der Liste der Mitgliedskonten/verknüpften Konten	Auflisten			

Von AWS Consolidated Billing definierte Ressourcen

AWS Consolidated Billing unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf AWS Consolidated Billing zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Consolidated Billing

Consolidated Billing besitzt keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Control Catalog

AWS Control Catalog (Dienstpräfix:`controlcatalog`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Durch AWS Control Catalog definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListCommonControls	Erteilt die Berechtigung, eine paginierte Liste gängiger Steuerelemente aus dem AWS Control Catalog zurückzugeben	Auflisten			
ListDomains	Erteilt die Erlaubnis, eine paginierte Liste von Domänen aus dem AWS Control Catalog zurückzugeben	Auflisten			
ListObjectives	Erteilt die Erlaubnis, eine paginierte Liste von Zielen aus dem AWS Kontrollkatalog zurückzugeben	Auflisten			

Im AWS Control Catalog definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
common-control	`arn:${Partition}:controlcatalog:::common-control/${CommonControlId}`	
domain	`arn:${Partition}:controlcatalog:::domain/${DomainId}`	
objective	`arn:${Partition}:controlcatalog:::objective/${ObjectiveId}`	

Bedingungsschlüssel für AWS Control Catalog

Control Catalog hat keine dienstspezifischen Kontextschlüssel, die im `Condition` Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Control Tower

AWS Control Tower (Dienstpräfix:`controltower`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.

- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Control Tower definierte Aktionen
- Von AWS Control Tower definierte Ressourcentypen
- Bedingungsschlüssel für AWS Control Tower

Von AWS Control Tower definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateLandingZone	Gewährt die Berechtigung zum Erstellen einer Landing Zone	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	controltower:TagResource
CreateManagedAccount [nur Berechtigung]	Erteilt die Erlaubnis, ein von AWS Control Tower verwaltetes Konto zu erstellen	Schreiben			
DeleteLandingZone	Erteilt die Erlaubnis, die landing zone des AWS Control Tower zu löschen	Schreiben	LandingZone*		
DeregisterManagedAccount [nur Berechtigung]	Erteilt die Erlaubnis, ein über die Account Factory erstelltes Konto von AWS Control Tower abzumelden	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeregisterOrganizationalUnit [nur Berechtigung]	Erteilt die Erlaubnis, eine Organisationseinheit von der AWS Control Tower Tower-Verwaltung abzumelden	Schreiben			
DescribeAccountFactoryConfig [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben der Konfiguration der aktuellen Account Factory	Lesen			
DescribeCoreService [nur Berechtigung]	Erteilt die Erlaubnis, Ressourcen zu beschreiben, die von Core-Konten in AWS Control Tower verwaltet werden	Lesen			
DescribeGuardrail [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben einesr Leitlinie	Lesen			
DescribeGuardrailForTarget [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben einer Leitlinie für eine Organisationseinheit	Lesen			
DescribeLandingZoneConfiguration [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben der aktuellen Konfiguration der Landing Zone	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeManagedAccount [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben eines Kontos, das über die Account Factory erstellt wurde	Lesen			
DescribeManagedOrganizationalUnit [nur Berechtigung]	Erteilt die Erlaubnis, eine vom AWS Control Tower verwaltete AWS Organisationseinheit einer Organisation zu beschreiben	Lesen			
DescribeRegisterOrganizationalUnitOperation [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben eines Vorgangs einer registrierten Organisationseinheit	Lesen			
DescribeSingleSignOn [nur Berechtigung]	Erteilt die Erlaubnis, die aktuelle AWS Control Tower IAM Identity Center-Konfiguration zu beschreiben	Lesen			
DisableBaseline	Erteilt die Erlaubnis, eine Baseline auf einem Ziel zu deaktivieren	Schreiben	EnabledBaseline*		
DisableControl	Gewährt die Berechtigung zum Entfernen einer Kontrolle aus einer Organisationseinheit	Schreiben	EnabledControl*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisableGuardrail [nur Berechtigung]	Gewährt die Berechtigung zum Deaktivieren eine Leitlinie von einer Organisationseinheit	Schreiben			
EnableBaseline	Erteilt die Berechtigung, eine Baseline auf einem Ziel zu aktivieren	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	controltower:TagResource
EnableControl	Erteilt die Berechtigung zum Aktivieren eines Steuerelements für eine Organisationseinheit	Schreiben	EnabledControl		controltower:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
EnableGuardrail [nur Berechtigung]	Gewährt die Berechtigung zum Aktivieren einer Leitlinie für eine Organisationseinheit	Schreiben			
GetAccountInfo [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben einer Konto-E-Mail-Adresse und Bestätigen ihres Vorhandenseins	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAvailableUpdates [nur Berechtigung]	Erteilt die Erlaubnis, verfügbare Updates für die aktuelle AWS Control Tower Tower-Bereitstellung aufzulisten	Lesen			
GetBaseline	Erteilt die Erlaubnis, Baseline-Details abzurufen	Lesen	Baseline*		
GetBaselineOperation	Erteilt die Berechtigung, den aktuellen Status eines bestimmten Baseline-Vorgangs abzurufen	Lesen			
GetControlOperation	Erteilt die Berechtigung, den aktuellen Status eines bestimmten DisableControl Vorgangs EnabledControl abzurufen	Lesen			
GetEnabledBaseline	Erteilt die Erlaubnis, eine aktivierte Baseline abzurufen	Lesen	EnabledBaseline*		
GetEnabledControl	Gewährt die Berechtigung zum Abrufen einer aktivierten Kontrolle aus einer Organisationseinheit	Lesen	EnabledControl*		
GetGuardrailComplianceStatus [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen des aktuellen Compliancestatus einer Leitlinie	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetHomeRegion [nur Berechtigung]	Erteilt die Erlaubnis, die Heimatregion des AWS Control Tower Tower-Setups abzurufen	Lesen			
GetLandingZone	Gewährt die Berechtigung zum Abrufen des aktuellen Status der Einrichtung der Landing Zone	Lesen	LandingZone*		
GetLandingZoneDriftStatus	Gewährt die Berechtigung zum Abrufen des aktuellen Abweichungsstatus der Landing Zone	Lesen			
GetLandingZoneOperation	Gewährt die Berechtigung zum Abrufen des aktuellen Status eines bestimmten Landing-Zone-Vorgangs	Lesen			
GetLandingZoneStatus [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen des aktuellen Status der Einrichtung der Landing Zone	Lesen			
ListBaselines	Erteilt die Erlaubnis, Baselines aufzulisten	Auflisten			
ListDirectoryGroups [nur Berechtigung]	Erteilt die Berechtigung, die aktuellen Verzeichnisgruppen aufzulisten, die über IAM Identity Center verfügbar sind	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDriftDetails	Erteilt die Erlaubnis, Drift-Vorkommen im AWS Control Tower aufzulisten	Lesen			
ListEnabledBaselines	Erteilt die Erlaubnis, aktivierte Baselines aufzulisten	Auflisten			
ListEnabledControls	Gewährt die Berechtigung zum Auflisten aller aktivierten Kontrollen in einer angegebenen Organisationseinheit	Auflisten			
ListEnabledGuardrails [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aktuell aktivierter Leitlinien	Auflisten			
ListExtendGovernancePrecheckDetails [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der Details von Vorabprüfungen für eine Organisationseinheit	Auflisten			
ListExternalConfigRuleCompliance	Erteilt die Erlaubnis, die Einhaltung externer AWS Konfigurationsregeln aufzulisten	Lesen			
ListGuardrailViolations [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten bestehender Leitlinienverstöße	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListGuardrails [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aller verfügbaren Leitlinien	Auflisten			
ListGuardrailsForTarget [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der Leitlinien und ihres aktuellen Status für eine Organisationseinheit	Auflisten			
ListLandingZones	Gewährt die Berechtigung zum Auflisten aller Landing Zone	Auflisten			
ListManagedAccounts [nur Berechtigung]	Erteilt die Erlaubnis, über AWS Control Tower verwaltete Konten aufzulisten	Auflisten			
ListManagedAccountsForGuardrail [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten verwalteter Konten mit einer bestimmten angewendeten Leitlinie	Auflisten			
ListManagedAccountsForParent [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten verwalteter Konten unter einer Organisationseinheit	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListManagedOrganizationalUnits [nur Berechtigung]	Erteilt die Erlaubnis, von AWS Control Tower verwaltete Organisationseinheiten aufzulisten	Auflisten			
ListManagedOrganizationalUnitsForGuardrail [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten verwalteter Organisationseinheiten, auf die eine bestimmte Leitlinie angewendet wurde	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für eine Ressource	Lesen	EnabledBaseline		
			EnabledControl		
			LandingZone		
ManageOrganizationalUnit [nur Berechtigung]	Erteilt die Erlaubnis, eine Organisationseinheit einzurichten, die von AWS Control Tower verwaltet werden soll	Schreiben			
PerformPreLaunchChecks [nur Berechtigung]	Gewährt die Berechtigung zum Ausführen von Bestätigungen in einem Konto	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ResetEnabledBaseline	Erteilt die Erlaubnis, eine aktivierte Baseline zurückzusetzen	Schreiben	EnabledBaseline*		
ResetLandingZone	Gewährt die Berechtigung zum Zurücksetzen einer Landing Zone	Schreiben	LandingZone*		
SetupLandingZone [nur Berechtigung]	Erteilt die Erlaubnis, die landing zone des AWS Control Tower einzurichten oder zu aktualisieren	Schreiben			
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Ressource	Markieren	EnabledBaseline		
			EnabledControl		
			LandingZone		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Ressource	Tagging	EnabledBaseline		
			EnabledControl		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			LandingZone		
				aws:TagKeys	
UpdateAccountFactoryConfig [nur Berechtigung]	Gewährt die Berechtigung, die Konfiguration der Account-Factory-Konfiguration zu aktualisieren	Schreiben			
UpdateEnabledBaseline	Erteilt die Erlaubnis, eine aktivierte Baseline zu aktualisieren	Schreiben	EnabledBaseline*		
UpdateEnabledControl	Gewährt die Berechtigung zum Aktualisieren einer aktivierten Kontrolle aus einer Organisationseinheit	Schreiben	EnabledControl*		
UpdateLandingZone	Gewährt die Berechtigung zum Aktualisieren einer Landing Zone	Schreiben	LandingZone*		

Von AWS Control Tower definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
EnabledControl	`arn:${Partition}:controltower:${Region}:${Account}:enabledcontrol/${EnabledControlId}`	aws:ResourceTag/${TagKey}
Baseline	`arn:${Partition}:controltower:${Region}::baseline/${BaselineId}`	
EnabledBaseline	`arn:${Partition}:controltower:${Region}:${Account}:enabledbaseline/${EnabledBaselineId}`	aws:ResourceTag/${TagKey}
LandingZone	`arn:${Partition}:controltower:${Region}:${Account}:landingzone/${LandingZoneId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Control Tower

AWS Control Tower definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Kosten- und Nutzungsbericht

AWS Cost and Usage Report (Servicepräfix: `cur`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS-Kosten- und Nutzungsbericht definierte Aktionen
- Von AWS Kosten- und Nutzungsbericht definierte Ressourcentypen
- Bedingungsschlüssel für AWS-Kosten- und Nutzungsbericht

Von AWS-Kosten- und Nutzungsbericht definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteReportDefinition	Gewährt die Berechtigung zum Löschen der „Cost and Usage Report“-Definition	Schreiben	cur*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeReportDefinitions	Gewährt die Berechtigung zum Erhalten der „Cost and Usage Report“-Definitionen	Lesen			
GetClassicReport [nur Berechtigung]	Gewährt die Berechtigung zum Erhalten des CSV-Berichts der Rechnung	Lesen			
GetClassicReportPreferences [nur Berechtigung]	Gewährt die Berechtigung zum Erhalten des klassischen Berichtsaktivierungsstatus für Nutzungsberichte	Lesen			
GetUsageReport [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der AWS-Services, des Nutzungstyps und des Vorgangs für den Arbeitsablauf „Nutzungsbericht“. Erlaubt oder verweigert auch das Herunterladen von Nutzungsberichten	Lesen			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen	cur*		
				aws:ResourceTag/${TagKey}	
ModifyReportDefinition	Gewährt die Berechtigung zum Ändern der „Cost and Usage Report“-Definition	Schreiben	cur*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutClassicReportPreferences [nur Berechtigung]	Gewährt die Berechtigung zum Aktivieren klassischer Berichte	Schreiben			
PutReportDefinition	Gewährt die Berechtigung zum Schreiben der „Cost and Usage Report“-Definition	Schreiben	cur*		
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren	cur*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Markieren	cur*		
				aws:TagKeys aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ValidateReportDestination [nur Berechtigung]	Gewährt die Berechtigung zum Überprüfen, ob der S3-Bucket existiert und über die entsprechenden Berechtigungen für die Bereitstellung des Kosten- und Nutzungsberichts verfügt	Lesen			

Von AWS Kosten- und Nutzungsbericht definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
cur	`arn:${Partition}:cur:${Region}:${Account}:definition/${ReportName}`	

Bedingungsschlüssel für AWS-Kosten- und Nutzungsbericht

Der AWS-Kosten- und Nutzungsbericht definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Cost Explorer Service

AWS Der Cost Explorer Explorer-Dienst (Dienstpräfix:`ce`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Cost Explorer Service definierte Aktionen
- Von AWS Cost Explorer Service definierte Ressourcentypen
- Bedingungsschlüssel für AWS Cost Explorer Service

Von AWS Cost Explorer Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAnomalyMonitor	Gewährt die Berechtigung zum Erstellen eines neuen Anomaliemonitors	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAnomalySubscription	Gewährt die Berechtigung zum Erstellen eines neuen Anomalieabonnements	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCostCategoryDefinition	Gewährt die Berechtigung zum Erstellen einer neuen Kostenkategorie mit dem angeforderten Namen und den Regeln	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateNotificationSubscription [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen von Warnungen beim Ablauf der Reservierung	Write			
CreateReport [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen von Cost Explorer-Berichten	Write			
DeleteAnomalyMonitor	Gewährt die Berechtigung zum Löschen eines Anomaliemonitors	Write	anomalymonitor*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
DeleteAnomalySubscription	Gewährt die Berechtigung zum Löschen eines Anomalieabonnements	Write	anomalysubscription*		
				aws:ResourceTag/${TagKey}	
DeleteCostCategoryDefinition	Gewährt die Berechtigung zum Löschen einer Kostenkategorie	Write	costcategory*		
				aws:ResourceTag/${TagKey}	
DeleteNotificationSubscription [nur Berechtigung]	Gewährt die Berechtigung zum Löschen von Warnungen beim Ablauf der Reservierung	Write			
DeleteReport [nur Berechtigung]	Gewährt die Berechtigung zum Löschen von Cost Explorer-Berichten	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeCostCategoryDefinition	Gewährt die Berechtigung zum Abrufen von Beschreibungen wie Name, ARN, Regeln, Definition und Gültigkeitsdaten einer Kostenkategorie	Read	costcategory*		
				aws:ResourceTag/${TagKey}	
DescribeNotificationSubscription [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen von Warnungen beim Ablauf der Reservierung	Read			
DescribeReport [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen der Seite für Cost Explorer-Berichte	Read			
GetAnomalies	Gewährt die Berechtigung zum Abrufen von Anomalien	Read	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
GetAnomalyMonitors	Gewährt die Berechtigung zum Abfragen von Anomaliemonitoren	Read	anomalymonitor*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAnomalySubscriptions	Gewährt die Berechtigung zum Abfragen von Anomaliea bonnements	Lesen	anomalysubscription*		
				aws:ResourceTag/${TagKey}	
GetApproximateUsageRecords	Gewährt die Berechtigung, die ungefähre Anzahl der Nutzungsdatensätze für die ausgewählten Ressourcen-, Level- und stündlichen Granularitätspräferenzen abzurufen, die aus der Nutzung des letzten Monats abgeleitet wurden	Lesen			
GetConsoleActionSetEnforced [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen, ob vorhandene oder detaillierte IAM-Aktionen verwendet werden, um die Autorisierung für die Fakturierungs-, Kostenmanagement- und Kontokonsolen zu steuern	Lesen			
GetCostAndUsage	Gewährt die Berechtigung zum Abrufen der Kosten und Nutzungsmetriken für Ihr Konto	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetCostAndUsageWithResources	Gewährt die Berechtigung zum Abrufen der Kosten und Nutzungsmetriken mit Ressourcen für Ihr Konto	Read			
GetCostCategories	Gewährt die Berechtigung zum Abfragen der Namen und Werte von Cost Categories für einen angegebenen Zeitraum	Read			
GetCostForecast	Gewährt die Berechtigung zum Abrufen einer Kostenschätzung für einen prognostizierten Zeitraum	Read			
GetDimensionValues	Gewährt die Berechtigung zum Abrufen aller verfügbaren Filterwerte eines Filters für einen bestimmten Zeitraum	Read			
GetPreferences [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen der Seite für Cost Explorer-Einstellungen	Read			
GetReservationCoverage	Gewährt die Berechtigung zum Abrufen der Reservierungsabdeckung für Ihr Konto	Lesen			
GetReservationPurchaseRecommendation	Gewährt die Berechtigung zum Abrufen der Reservierungsempfehlungen für Ihr Konto	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetReservationUtilization	Gewährt die Berechtigung zum Abrufen der Reservierungsauslastung für Ihr Konto	Read			
GetRightsizingRecommendation	Gewährt die Berechtigung zum Abrufen der Rightsizing-Empfehlungen für Ihr Konto	Lesen			
GetSavingsPlanPurchaseRecommendationDetails	Gewährt die Berechtigung zum Abrufen der Empfehlungsdetails für Savings Plans für Ihr Konto	Lesen			
GetSavingsPlansCoverage	Gewährt die Berechtigung zum Abrufen der Savings Plans für Ihr Konto	Read			
GetSavingsPlansPurchaseRecommendation	Gewährt die Berechtigung zum Abrufen der Empfehlungen für Savings Plans für Ihr Konto	Read			
GetSavingsPlansUtilization	Gewährt die Berechtigung zum Abrufen der Savings Plans-Nutzung für Ihr Konto	Read			
GetSavingsPlansUtilizationDetails	Gewährt die Berechtigung zum Abrufen Savings Plans-Nutzungsdetails für Ihr Konto	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetTags	Gewährt die Berechtigung zum Abfragen von Tags für einen bestimmten Zeitraum	Read			
GetUsageForecast	Gewährt die Berechtigung zum Abrufen einer Nutzungsschätzung für einen prognostizierten Zeitraum	Lesen			
ListCostAllocationTagBackfillHistory	Erteilt die Berechtigung, die Auffüllhistorie für das Cost Allocation Tag aufzulisten	Auflisten			
ListCostAllocationTags	Gewährt die Berechtigung zum Auflisten aller Kostenzuordnungs-Tags	Auflisten			
ListCostCategoryDefinitions	Gewährt die Berechtigung zum Abrufen von Namen, ARN und Gültigkeitsdaten für alle Cost Categories	Auflisten			
ListSavingsPlansPurchaseRecommendationGeneration	Gewährt die Berechtigung zum Abrufen einer Liste Ihrer historischen Empfehlungsgenerationen	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags einer Cost Explorer-Ressource	Lesen	anomalymonitor		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			anomalysubscription		
			costcategory		
				aws:ResourceTag/${TagKey}	
ProvideAnomalyFeedback	Gewährt die Berechtigung, Feedback zu erkannten Anomalien zu geben	Schreiben			
StartCostAllocationTagBackfill	Erteilt die Erlaubnis, eine Auffüllung mit dem Cost Allocation Tag anzufordern	Schreiben			
StartSavingsPlansPurchaseRecommendationGeneration	Gewährt die Berechtigung zum Anfordern der Generierung einer Empfehlung für Savings Plans	Schreiben			
TagResource	Gewährt die Berechtigung zum Taggen einer Cost Explorer-Ressource	Tagging	anomalymonitor		
			anomalysubscription		
			costcategory		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Cost Explorer-Ressource	Tagging	anomalymonitor		
			anomalysubscription		
			costcategory		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateAnomalyMonitor	Gewährt die Berechtigung zum Aktualisieren eines vorhandenen Anomaliemonitors	Write	anomalymonitor*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateAnomalySubscription	Gewährt die Berechtigung zum Aktualisieren eines vorhandenen Anomaliea bonnements	Schreiben	anomalysubscription*		
				aws:ResourceTag/${TagKey}	
UpdateConsoleActionSetEnforced [nur Berechtigung]	Gewährt die Berechtigung zum Ändern, ob vorhanden e oder detaillierte IAM-Aktio nen verwendet werden sollen, um die Autorisierung für die Fakturierungs-, Kostenman agement- und Kontokonsolen zu steuern	Schreiben			
UpdateCostAllocationTagsStatus	Gewährt die Berechtigung zum Aktualisieren vorhanden er Kostenzuordnungs-Tags-Status	Schreiben			
UpdateCostCategoryDefinition	Gewährt die Berechtigung zur Aktualisierung einer vorhandenen Kostenkategorie	Write	costcategory*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateNotificationSubscription [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren von Warnungen beim Ablauf der Reservierung	Write			
UpdatePreferences [nur Berechtigung]	Gewährt die Berechtigung zum Bearbeiten der Seite für Cost Explorer-Einstellungen	Write			
UpdateReport [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren von Cost Explorer-Berichten	Write			

Von AWS Cost Explorer Service definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
anomalysubscription	`arn:${Partition}:ce::${Account}:anomalysubscription/${Identifier}`	aws:ResourceTag/${TagKey}
anomalymonitor	`arn:${Partition}:ce::${Account}:anomalymonitor/${Identifier}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
costcategory	`arn:${Partition}:ce::${Account}:costcategory/${Identifier}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Cost Explorer Service

AWS Der Cost Explorer Explorer-Dienst definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Cost Optimization Hub

AWS Cost Optimization Hub (Servicepräfix: `cost-optimization-hub`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Cost Optimization Hub definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetPreferences	Gewährt die Berechtigung zum Abrufen von Präferenzen	Lesen			
GetRecommendation	Gewährt die Berechtigung, die Ressourcenkonfiguration und die geschätzten Kostenauswirkungen für eine Empfehlung abzurufen	Lesen			
ListEnrollmentStatuses	Gewährt die Berechtigung, den Anmeldestatus für das angegebene Konto oder für alle Mitglieder eines Verwaltungskontos aufzulisten	Auflisten			
ListRecommendationSummaries	Gewährt die Berechtigung zum Auflisten von Empfehlungszusammenfassungen nach Gruppen	Auflisten			cost-optimization-hub:GetRecommendation

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListRecommendations	Gewährt die Berechtigung eine Zusammenfassung der Empfehlungen aufzulisten	Auflisten			cost-optimization-hub:GetRecommendation
UpdateEnrollmentStatus	Gewährt die Berechtigung zum Aktualisieren des Registrierungsstatus	Schreiben			
UpdatePreferences	Gewährt die Berechtigung zum Aktualisieren von Präferenzen	Schreiben			

Von AWS Cost Optimization Hub definierte Ressourcentypen

AWS Cost Optimization Hub unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`Element einer IAM-Richtlinienanweisung. Um den Zugriff auf AWS Cost Optimization Hub zu ermöglichen, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Zustandsschlüssel für AWS Cost Optimization Hub

Cost Optimization Hub besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Customer Verification Service

AWS Customer Verification Service (Servicepräfix: `customer-verification`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Vom AWS Customer Verification Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCustomerVerificationDetails [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen von Kundenprüfdaten	Schreiben			
GetCustomerVerificationDetails [nur Berechtigung]	Gewährt die Berechtigung zum Erhalt von Kundenprüfdaten	Lesen			
GetCustomerVerificationEligibility [nur Berechtigung]	Gewährt die Berechtigung, die Voraussetzungen für die Kundenprüfung zu erhalten	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateCustomerVerificationDetails [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren von Kundenprüfdaten	Schreiben			

Vom AWS Customer Verification Service definierte Ressourcentypen

AWS Customer Verification Service unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf den AWS Customer Verification Service zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für den AWS Customer Verification Service

Customer Verification Service umfasst keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Data Exchange

AWS Data Exchange (Servicepräfix: `dataexchange`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Data Exchange definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelJob	Gewährt die Berechtigung zum Abbrechen einer Aufgabe.	Schreiben	jobs*		
CreateAsset [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer Komponente (z. B. in einem Auftrag)	Schreiben	revisions*		
CreateDataSet	Gewährt die Berechtigung zum Erstellen eines neuen Datasets	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventAction	Gewährt die Berechtigung zum Erstellen einer Ereignisaktion	Schreiben			
CreateJob	Gewährt die Berechtigung zum Erstellen eines Auftrags zum Importieren oder Exportieren von Komponenten	Schreiben			
CreateRevision	Gewährt die Berechtigung zum Erstellen einer Überarbeitung	Schreiben	data-sets*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAsset	Gewährt die Berechtigung zum Löschen einer Komponente	Schreiben	assets*		
DeleteDataSet	Gewährt die Berechtigung zum Löschen eines Datasets	Schreiben	data-sets*		
			entitled-data-sets*		
DeleteEventAction	Gewährt die Berechtigung zum Löschen einer Ereignisaktion	Schreiben	event-actions*		
DeleteRevision	Gewährt die Berechtigung zum Löschen einer Revision	Schreiben	revisions*		
GetAsset	Gewährt die Berechtigung zum Abrufen von Informationen über eine Komponente und zum Exportieren der Komponente (z. B. in einem Auftrag)	Lesen	assets*		
			entitled-assets*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDataSet	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Dataset	Lesen	data-sets*		
			entitled-data-sets*		
GetEventAction	Gewährt die Berechtigung zum Erhalten einer Ereignisaktion	Lesen	event-actions*		
GetJob	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Auftrag	Lesen	jobs*		
GetRevision	Gewährt die Berechtigung zum Abrufen von Informationen über eine Überarbeitung	Lesen	entitled-revisions*		
			revisions*		
ListDataSetRevisions	Gewährt die Berechtigung zum Auflisten der Revisionen eines Datasets	Auflisten	data-sets*		
			entitled-data-sets*		
ListDataSets	Gewährt die Berechtigung zum Auflisten von Datasets für das Konto	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListEventActions	Gewährt die Berechtigung zum Auflisten von Ereignisaktionen für das Konto	Auflisten			
ListJobs	Gewährt die Berechtigung zum Auflisten von Aufträgen für das Konto	Auflisten			
ListRevisionAssets	Gewährt die Berechtigung zum Abrufen der Liste der Komponenten einer Revision	Auflisten	entitled-revisions*		
			revisions*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags, die Sie mit der angegebenen Ressource verknüpft haben	Auflisten	data-sets		
			revisions		
PublishDataSet [nur Berechtigung]	Gewährt die Berechtigung zum Veröffentlichen eines Datensatzes	Schreiben	data-sets*		
RevokeRevision	Gewährt die Berechtigung, den Zugriff des Subscribers auf eine Revision zu widerrufen	Schreiben	revisions*		
SendApiAsset	Gewährt die Berechtigung zum Senden einer Anfrage an eine API-Komponente	Schreiben	assets*		
			entitled-assets*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SendDataSetNotification	Gewährt die Berechtigung zum Senden einer Benachrichtigung an Subscriber eines Datensatzes	Schreiben	data-sets*		
StartJob	Gewährt die Berechtigung zum Starten eines Auftrags	Schreiben	jobs*		dataexchange:CreateAsset dataexchange:DeleteDataSet dataexchange:GetAsset dataexchange:GetDataSet dataexchange:GetRevision dataexchange:PublishDataSet redshift:AuthorizeDataShare

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Tags zu einer bestimmten Ressource	Markieren	data-sets		
			revisions		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen eines oder mehrerer Tags von einer bestimmten Ressource	Markierung	data-sets		
			revisions		
				aws:TagKeys	
UpdateAsset	Gewährt die Berechtigung zum Abrufen von Aktualisierungsinformationen zu einer Komponente	Schreiben	assets*		
UpdateDataSet	Gewährt die Berechtigung zum Aktualisieren von Informationen zu einem Dataset	Schreiben	data-sets*		
UpdateEventAction	Gewährt die Berechtigung zum Aktualisieren der von Informationen zu einer Ereignisaktion	Schreiben	event-actions*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateRevision	Gewährt die Berechtigung zum Aktualisieren von Informationen zu einer Revision	Schreiben	revisions *		dataexchange:PublishDataSet

Von AWS Data Exchange definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
jobs	`arn:${Partition}:dataexchange:${Region}:${Account}:jobs/${JobId}`	dataexchange:JobType
data-sets	`arn:${Partition}:dataexchange:${Region}:${Account}:data-sets/${DataSetId}`	aws:ResourceTag/${TagKey}
entitled-data-sets	`arn:${Partition}:dataexchange:${Region}::data-sets/${DataSetId}`	
revisions	`arn:${Partition}:dataexchange:${Region}:${Account}:data-sets/${DataSetId}/revisions/${RevisionId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
entitled-revisions	`arn:${Partition}:dataexchange:${Region}::data-sets/${DataSetId}/revisions/${RevisionId}`	
assets	`arn:${Partition}:dataexchange:${Region}:${Account}:data-sets/${DataSetId}/revisions/${RevisionId}/assets/${AssetId}`	
entitled-assets	`arn:${Partition}:dataexchange:${Region}::data-sets/${DataSetId}/revisions/${RevisionId}/assets/${AssetId}`	
event-actions	`arn:${Partition}:dataexchange:${Region}:${Account}:event-actions/${EventActionId}`	

Bedingungsschlüssel für AWS Data Exchange

AWS Data Exchange definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem zulässigen Satz von Werten für jedes der obligatorischen Tags in der Erstellungsanforderung	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Tag-Wert, der der Ressource zugeordnet ist	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach dem Vorhandensein verbindlicher Tags in der Erstellungsanforderung	ArrayOfString
dataexchange:JobType	Filtert den Zugriff nach dem angegebenen Auftragstyp	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Data Lifecycle Manager

Amazon Data Lifecycle Manager (Servicepräfix: `dlm`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Data Lifecycle Manager definierte Aktionen
- Von Amazon Data Lifecycle Manager definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Data Lifecycle Manager

Von Amazon Data Lifecycle Manager definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen.

Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateLifecyclePolicy	Gewährt die Berechtigung, eine Richtlinie für den Datenlebenszyklus zu erstellen, um die geplante Erstellung und Aufbewahrung von Amazon-EBS-Snapshots zu verwalten. Sie können bis zu 100 Richtlinien haben.	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteLifecyclePolicy	Gewährt die Berechtigung, eine vorhandene Richtlinie für den Datenlebenszyklus zu löschen Darüber hinaus können Sie mit dieser Aktion die Erstellung und Löschung von Snapshots anhalten, die in der Richtlinie angegeben sind. Vorhandene Snapshots sind nicht betroffen	Schreiben	policy*		
GetLifecyclePolicies	Gewährt die Berechtigung, eine Liste der zusammenfassenden Beschreibungen der Richtlinien für den Datenlebenszyklus zurückzugeben	Auflisten			
GetLifecyclePolicy	Gewährt die Berechtigung, eine vollständige Beschreibung einer einzelnen Richtlinie für den Datenlebenszyklus zurückzugeben	Lesen	policy*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags, die einer Ressource zugeordnet sind	Lesen	policy*		
TagResource	Gewährt die Berechtigung zum Hinzufügen oder Aktualisieren von Tags einer Ressource	Markierung	policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags, die einer Ressource zugeordnet sind.	Markierung	policy*		
				aws:TagKeys	
UpdateLifecyclePolicy	Gewährt die Berechtigung, eine vorhandene Richtlinie für den Datenlebenszyklus zu aktualisieren	Schreiben	policy*		

Von Amazon Data Lifecycle Manager definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
policy	`arn:${Partition}:dlm:${Region}:${Account}:policy/${ResourceName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Data Lifecycle Manager

Amazon Data Lifecycle Manager definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüsselwertpaaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Data Pipeline

AWS Data Pipeline (Servicepräfix: `datapipeline`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Data Pipeline definierte Aktionen
- Von AWS Data Pipeline definierte Ressourcentypen
- Bedingungsschlüssel für AWS Data Pipeline

Von AWS Data Pipeline definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ActivatePipeline	Gewährt die Berechtigung zum Validieren der angegebenen Pipeline und Starten der Verarbeitung der Pipeline-Aufgaben. Wenn die Pipeline nicht validiert werden kann, schlägt die Aktivierung fehl.	Schreiben	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag datapipeline:workerGroup	
AddTags	Gewährt die Berechtigung zum Hinzufügen oder Ändern von Tags für die angegebene Pipeline	Markierung	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePipeline	Gewährt die Berechtigung zum Erstellen einer neuen, leeren Pipeline	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys datapipeline:Tag	datapipeline:AddTags
DeactivatePipeline	Gewährt die Berechtigung zum Deaktivieren der angegebenen laufenden Pipeline	Schreiben	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag datapipeline:workerGroup	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeletePipeline	Gewährt die Berechtigung zum Löschen einer Pipeline, ihrer Definition und ihres Ausführungsverlaufs	Schreiben	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag	
DescribeObjects	Gewährt die Berechtigung zum Abrufen der Objektdefinitionen für einen Satz der Pipeline zugeordneter Objekte	Lesen	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag	
DescribePipelines	Gewährt die Berechtigung zum Abrufen der Metadaten einzelner oder mehrerer Pipelines	Lesen	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
EvaluateExpression	Gewährt Task Runnern die Berechtigung zum Aufruf von EvaluateExpression, um eine Zeichenfolge im Kontext des angegebenen Objekts auszuwerten	Lesen	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag	
GetAccountLimits [nur Berechtigung]	Gewährt die Berechtigung zum Aufrufen von GetAccountLimits	Auflisten			
GetPipelineDefinition	Gewährt die Berechtigung zum Abrufen der Definition der angegebenen Pipeline	Lesen	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag datapipeline:workerGroup	
ListPipelines	Gewährt die Berechtigung zum Auflisten der Pipeline-IDs für alle aktiven Pipelines, auf die Sie zugreifen dürfen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PollForTask	Gewährt Task Runnern die Berechtigung zum Aufruf von PollForTask, um eine auszuführende Aufgabe von AWS Data Pipeline zu empfangen	Schreiben		datapipeline:workerGroup	
PutAccountLimits [nur Berechtigung]	Gewährt die Berechtigung zum Aufrufen von PutAccountLimits	Schreiben			
PutPipelineDefinition	Gewährt die Berechtigung zum Hinzufügen von Aufgaben, Zeitplänen und Voraussetzungen zur angegebenen Pipeline	Schreiben	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag datapipeline:workerGroup	
QueryObjects	Gewährt die Berechtigung zur Abfrage der angegebenen Pipeline nach Namen der Objekte, die den angegebenen Bedingungen entsprechen	Lesen	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RemoveTags	Gewährt die Berechtigung zum Entfernen von Tags aus der angegebenen Pipeline	Markierung	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag aws:TagKeys aws:RequestTag/${TagKey}	
ReportTaskProgress	Gewährt Task Runnern die Berechtigung zum Aufruf von ReportTaskProgress, nachdem eine Aufgabe zugewiesen wurde, um den Erhalt der Aufgabe zu bestätigen	Schreiben	pipeline*		
ReportTaskRunnerHeartbeat	Gewährt Task Runnern die Berechtigung zum Aufruf von ReportTaskRunnerHeartbeat alle 15 Minuten, um Betriebsbereitschaft zu melden	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SetStatus	Gewährt die Berechtigung zur Abfrage des Status der angegebenen physischen oder virtuellen Pipeline-Objekte in der angegebenen Pipeline	Schreiben	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag	
SetTaskStatus	Gewährt Task Runnern die Berechtigung zum Aufruf von SetTaskStatus, um AWS Data Pipeline darüber zu benachrichtigen, dass eine Aufgabe abgeschlossen wurde, und um Informationen über den abschließenden Status bereitzustellen	Schreiben	pipeline*		
ValidatePipelineDefinition	Gewährt die Berechtigung zur Validierung der angegebenen Pipeline-Definition, um sicherzustellen, dass diese richtig strukturiert ist und ohne Fehler ausgeführt werden kann	Lesen	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag datapipeline:workerGroup	

Von AWS Data Pipeline definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
pipeline	`arn:${Partition}:datapipeline:${Region}:${Account}:pipeline/${PipelineId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Data Pipeline

AWS Data Pipeline definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString
datapipeline:PipelineCreator	Filtert den Zugriff nach dem IAM-Benutzer, der die Pipeline erstellt hat	ArrayOfString
datapipeline:Tag	Filtert den Zugriff nach einem kundenspezifischen Schlüssel/Wert-Paar, das einer Ressource angefügt werden kann	ArrayOfString
datapipeline:workerGroup	Filtert den Zugriff nach dem Namen der Workergruppe, für die ein Task Runner Aufträge abruft	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Database Migration Service

AWS Database Migration Service (Servicepräfix: dms) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Database Migration Service definierte Aktionen
- Von AWS Database Migration Service definierte Ressourcentypen
- Bedingungsschlüssel für AWS Database Migration Service

Von AWS Database Migration Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWSzu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddTagsToResource	Gewährt die Berechtigung zum Hinzufügen von Metadaten-Tags zu DMS-Ressourcen, darunter Replikations-Instances, Endpunkte, Sicherheitsgruppen und Migrationsaufgaben	Markieren	Certificate		
			DataMigration		
			DataProvider		
			Endpoint		
			EventSubscription		
			InstanceProfile		
			MigrationProject		
			ReplicationConfig		
			ReplicationInstance		
			ReplicationSubnetGroup		
			ReplicationTask		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
ApplyPendingMaintenanceAction	Gewährt die Berechtigung zur Anwendung einer ausstehenden Wartungsaktion auf eine Ressource (z. B. eine Replikations-Instance)	Schreiben	ReplicationInstance*		
AssociateExtensionPack	Gewährt die Berechtigung zum Zuordnen eines Erweiterungspakets	Schreiben	MigrationProject*		dms:StartExtensionPackAssociation
BatchStartRecommendations	Gewährt die Berechtigung zum Starten der Analyse von bis zu 20 Quelldatenbanken, um Ziel-Engines für jede Quelldatenbank zu empfehlen	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelMetadataModelAssessment	Gewährt die Berechtigung zum Abbrechen einer einzelnen Metadatenmodell-Bewertungsausführung	Schreiben	MigrationProject*		
CancelMetadataModelConversion	Gewährt die Berechtigung zum Abbrechen eines einzigen Konvertierungslaufs eines Metadatenmodells	Schreiben	MigrationProject*		
CancelMetadataModelExport	Gewährt die Berechtigung zum Abbrechen eines einzigen Metadatenmodellexportlaufs	Schreiben	MigrationProject*		
CancelReplicationTaskAssessmentRun	Gewährt die Berechtigung, einen einzigen Bewertungslauf vor der Migration abzubrechen	Schreiben	ReplicationTaskAssessmentRun*		
CreateDataMigration	Gewährt die Berechtigung zum Erstellen einer Datenbankmigration mit den bereitgestellten Einstellungen	Schreiben	MigrationProject*		iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
CreateDataProvider	Gewährt die Berechtigung zum Erstellen eines Datenanbieters mit den bereitgestellten Einstellungen	Schreiben		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateEndpoint	Gewährt die Berechtigung zum Erstellen eines Endpunkts mit den bereitgestellten Einstellungen	Schreiben		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole
CreateEventSubscription	Gewährt die Berechtigung zum Erstellen eines AWS -DMS-Ereignisbenachrichtigungsabonnements	Schreiben		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateFleetAdvisorCollector	Gewährt die Berechtigung, einen Fleet-Advisor-Collector mit den angegebenen Parametern zu erstellen	Schreiben			iam:PassRole
CreateInstanceProfile	Gewährt die Berechtigung zum Erstellen eines Instance-Profils mit den bereitgestellten Einstellungen	Schreiben		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole
CreateMigrationProject	Gewährt die Berechtigung zum Erstellen eines Migrationsprojekts mit den bereitgestellten Einstellungen	Schreiben	DataProvider* InstanceProfile*		iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
CreateReplicationConfig	Gewährt die Berechtigung zum Erstellen einer Replikationskonfiguration mit den bereitgestellten Einstellungen	Schreiben	Endpoint*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateReplicationInstance	Gewährt die Berechtigung zum Erstellen einer Replikations-Instance unter Verwendung der angegebenen Parameter	Write		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole
CreateReplicationSubnetGroup	Gewährt die Berechtigung zum Erstellen einer Replikations-Subnetzgruppe für eine Liste der Subnetz-IDs in einer VPC	Write		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateReplicationTask	Gewährt die Berechtigung zum Erstellen einer Replikationsaufgabe mit den angegebenen Parametern	Write	Endpoint*		
			ReplicationInstance*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
DeleteCertificate	Gewährt die Berechtigung zum Löschen des angegebenen Zertifikats	Write	Certificate*		
DeleteConnection	Gewährt die Berechtigungen zum Löschen der angegebenen Verbindung zwischen einer Replikations-Instance und einem Endpunkt	Schreiben	Endpoint*		
			ReplicationInstance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteDataMigration	Gewährt die Berechtigung zum Löschen der angegebenen Datenbankmigration	Schreiben	DataMigration*		
DeleteDataProvider	Gewährt die Berechtigung zum Löschen des angegebenen Datenanbieters	Schreiben	DataProvider*		
DeleteEndpoint	Gewährt die Berechtigung zum Löschen des angegebenen Endpunkts	Schreiben	Endpoint*		
DeleteEventSubscription	Gewährt die Berechtigung zum Löschen eines AWS -DMS-Ereignisabonnements	Schreiben	EventSubscription*		
DeleteFleetAdvisorCollector	Gewährt die Berechtigung zum Löschen des angegebenen Fleet-Advisor-Collector	Schreiben			
DeleteFleetAdvisorDatabases	Gewährt die Berechtigung zum Löschen der angegebenen Fleet-Advisor-Datenbanken	Schreiben			
DeleteInstanceProfile	Gewährt die Berechtigung zum Löschen des angegebenen Instance-Profils.	Schreiben	InstanceProfile*		
DeleteMigrationProject	Gewährt die Berechtigung zum Löschen des angegebenen Migrationsprojekts	Schreiben	MigrationProject*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteReplicationConfig	Gewährt die Berechtigung zum Löschen der angegebenen Replikationskonfiguration	Schreiben	ReplicationConfig*		
DeleteReplicationInstance	Gewährt die Berechtigung zum Löschen der angegebenen Replikations-Instance	Write	ReplicationInstance*		
DeleteReplicationSubnetGroup	Gewährt die Berechtigung zum Löschen einer Subnetzgruppe	Write	ReplicationSubnetGroup*		
DeleteReplicationTask	Gewährt die Berechtigung zum Löschen der angegebenen Replikationsaufgabe	Write	ReplicationTask*		
DeleteReplicationTaskAssessmentRun	Gewährt die Berechtigung, den Datensatz eines einzelnen Bewertungslaufs vor der Migration zu löschen	Schreiben	ReplicationTaskAssessmentRun*		
DescribeAccountAttributes	Gewährt die Berechtigung zum Auflisten aller AWS DMS-Attribute für ein Kundenkonto	Lesen			
DescribeApplicableIndividualAssessments	Gewährt die Berechtigung zum Auflisten einzelner Bewertungen, die Sie für einen neuen Bewertungslauf vor der Migration angeben können	Read	ReplicationInstance		
			ReplicationTask		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeCertificates	Gewährt die Berechtigung, eine Beschreibung des Zertifikats bereitzustellen	Read			
DescribeConnections	Gewährt die Berechtigung, den Status der Verbindungen zwischen der Replikations-Instance und einem Endpunkt zu beschreiben	Lesen			
DescribeConversionConfiguration	Gewährt die Berechtigung, Informationen zur Projektkonfiguration der DMS-Schemakonvertierung zurückzugeben	Lesen	MigrationProject*		
DescribeDataMigrations	Gewährt die Berechtigung, Informationen zu Datenbankmigrationen für Ihr Konto in der angegebenen Region zurückzugeben	Lesen			
DescribeDataProviders [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der AWS DMS-Attribute für einen Datenanbieter. Hinweis: Diese Aktion sollte zusammen mit hinzugefügt werden ListDataProviders, autorisiert derzeit jedoch nicht den beschriebenen Schemakonvertierungsvorgang	Lesen	DataProvider		dms:ListDataProviders

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeEndpointSettings	Gewährt die Berechtigung, die möglichen Endpunkteinstellungen zurückzugeben, die beim Erstellen eines Endpunkts für ein bestimmtes Datenbankmodul verfügbar sind	Lesen			
DescribeEndpointTypes	Gewährt die Berechtigung, Informationen zum Typ der verfügbaren Endpunkte zurückzugeben	Read			
DescribeEndpoints	Gewährt die Berechtigung, Informationen zu den Endpunkten für Ihr Konto in der aktuellen Region zurückzugeben	Lesen			
DescribeEngineVersions	Gewährt die Berechtigung zum Zurückgeben von Informationen zu den verfügbaren Versionen für DMS-Replikations-Instances	Lesen			
DescribeEventCategories	Gewährt die Berechtigung, Kategorien für alle Ereignisquelltypen oder – falls angegeben – für einen angegebenen Quelltyp aufzulisten	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeEventSubscriptions	Gewährt die Berechtigung zum Auflisten aller Ereignisabonnements für ein Kundenkonto	Read			
DescribeEvents	Gewährt die Berechtigung zum Auflisten von Ereignissen für eine bestimmte Quell-ID und einen bestimmten Quelltyp	Lesen			
DescribeExtensionPackAssociations [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der AWS DMS-Attribute für Erweiterungspakete. Hinweis: Diese Aktion sollte zusammen mit hinzugefügt werden ListExtensionPacks, autorisiert derzeit jedoch nicht den beschriebenen Schemakonvertierungsvorgang	Lesen	Migration Project*		dms:ListExtensionPacks
DescribeFleetAdvisorCollectors	Gewährt die Berechtigung, basierend auf Filtereinstellungen eine paginierte Liste von Fleet-Advisor-Collectors in Ihrem Konto zurückzugeben	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeFleetAdvisorDatabases	Gewährt die Berechtigung, basierend auf Filtereinstellungen eine paginierte Liste von Fleet-Advisor-Datenbanken in Ihrem Konto zurückzugeben	Lesen			
DescribeFleetAdvisorLsaAnalysis	Gewährt die Berechtigung, eine paginierte Liste mit Beschreibungen von LSA (large-scale assessment)-Analysen zurückzugeben, die von Ihren Fleet-Advisor-Collectors erstellt wurden	Lesen			
DescribeFleetAdvisorSchemaObjectSummary	Gewährt die Berechtigung, basierend auf Filtereinstellungen eine paginierte Liste mit Beschreibungen der von Ihren Fleet-Advisor-Collectors entdeckten Schemata zurückzugeben	Lesen			
DescribeFleetAdvisorSchemas	Gewährt die Berechtigung, basierend auf Filtereinstellungen eine paginierte Liste der von Ihren Fleet-Advisor-Collectors entdeckten Schemata zurückzugeben	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeInstanceProfiles [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der AWS DMS-Attribute für ein Instance-Profil. Hinweis: Diese Aktion sollte zusammen mit hinzugefügt werden ListInstanceProfiles, autorisiert derzeit jedoch nicht den beschriebenen Schemakonvertierungsvorgang	Lesen	InstanceProfile		dms:ListInstanceProfiles
DescribeMetadataModelAssessments [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der AWS DMS-Attribute für Metadatenmodellbewertungen. Hinweis: Diese Aktion sollte zusammen mit hinzugefügt werden ListMetadataModelAssessments, autorisiert derzeit jedoch nicht den beschriebenen Schemakonvertierungsvorgang	Lesen	Migration Project*		dms:ListMetadataModelAssessments

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeMetadataModelConversions [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der AWS DMS-Attribute für eine Metadatenmodellkonvertierung. Hinweis: Diese Aktion sollte zusammen mit hinzugefügt werden ListMetadataModelConversions, autorisiert derzeit jedoch nicht den beschriebenen Schemakonvertierungsvorgang	Lesen	Migration Project*		dms:ListMetadataModelConversions
DescribeMetadataModelExportsAsScript [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der AWS DMS-Attribute für einen Metadatenmodellexport. Hinweis: Diese Aktion sollte zusammen mit hinzugefügt werden ListMetadataModelExports, autorisiert derzeit jedoch nicht den beschriebenen Schemakonvertierungsvorgang	Lesen	Migration Project*		dms:ListMetadataModelExports

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeMetadataModelExportsToTarget [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der AWS DMS-Attribute für einen Metadatenmodellexport. Hinweis: Diese Aktion sollte zusammen mit hinzugefügt werden ListMetadataModelExports, autorisiert derzeit jedoch nicht den beschriebenen Schemakonvertierungsvorgang	Lesen	MigrationProject*		dms:ListMetadataModelExports
DescribeMetadataModelImports	Gewährt die Berechtigung, Informationen über Startvorgänge von Metadatenmodellimporten für ein Migrationsprojekt zurückzugeben	Lesen	MigrationProject*		
DescribeMigrationProjects [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der AWS DMS-Attribute für ein Migrationsprojekt. Hinweis: Diese Aktion sollte zusammen mit hinzugefügt werden ListMigrationProjects, autorisiert derzeit jedoch nicht den beschriebenen Schemakonvertierungsvorgang	Lesen	DataProvider		dms:ListMigrationProjects
			InstanceProfile		
			MigrationProject		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeOrderableReplicationInstances	Gewährt die Berechtigung, Informationen zu den Replikations-Instance-Typen zurückzugeben, die in der angegebenen Region erstellt werden können	Lesen			
DescribePendingMaintenanceActions	Gewährt die Berechtigung zum Zurückgeben von Informationen zu ausstehenden Wartungsaktionen	Lesen			
DescribeRecommendationLimitations	Gewährt die Berechtigung zum Zurückgeben einer paginierten Liste von Beschreibungen der Einschränkungen für Empfehlungen von Ziel- AWS Engines	Lesen			
DescribeRecommendations	Gewährt die Berechtigung zum Zurückgeben einer paginierten Liste mit Beschreibungen der Empfehlungen von Ziel-Engines für Ihre Quelldatenbanken	Lesen			
DescribeRefreshSchemasStatus	Gewährt die Berechtigung zum Zurückgeben des Status der RefreshSchemas Operation	Lesen	Endpoint*		
DescribeReplicationConfigs	Gewährt die Berechtigung zum Beschreiben der Replikationskonfiguration	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeReplicationInstanceTaskLogs	Gewährt die Berechtigung, Informationen zu den Aufgabenprotokollen für die angegebene Aufgabe zurückzugeben	Read	ReplicationInstance*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
DescribeReplicationInstances	Gewährt die Berechtigung, Informationen zu Replikations-Instances für Ihr Konto in der aktuellen Region zurückzugeben	Read			
DescribeReplicationSubnetGroups	Gewährt die Berechtigung, Informationen zu den Replikationssubnetzgruppen zurückzugeben	Lesen			
DescribeReplicationTableStatistics	Gewährt die Berechtigung zum Beschreiben von Replikationstabellenstatistiken	Lesen	ReplicationConfig*		
DescribeReplicationTaskAssessmentResults	Gewährt die Berechtigung, die neuesten Ergebnisse der Aufgabenbewertung von Amazon S3 zurückzugeben	Read	ReplicationTask		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeReplicationTaskAssessmentRuns	Gewährt die Berechtigung, eine paginierte Liste von Bewertungsläufen vor der Migration zurückzugeben, die auf Filtereinstellungen basieren	Read	ReplicationInstance		
			ReplicationTask		
			ReplicationTaskAssessmentRun		
DescribeReplicationTaskIndividualAssessments	Gewährt die Berechtigung, eine paginierte Liste einzelner Bewertungen zurückzugeben, die auf Filtereinstellungen basieren	Read	ReplicationTask		
			ReplicationTaskAssessmentRun		
DescribeReplicationTasks	Gewährt die Berechtigung, Informationen zu Replikationsaufgaben für Ihr Konto in der aktuellen Region zurückzugeben	Lesen			
DescribeReplications	Gewährt die Berechtigung zum Beschreiben von Replikationen	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeSchemas	Gewährt die Berechtigung, Informationen zum Schema für den angegebenen Endpunkt zurückzugeben	Read	Endpoint*		
DescribeTableStatistics	Gewährt die Berechtigung, Tabellenstatistiken zur Datenbankmigrationsaufgabe zurückzugeben, einschließlich Tabellenname, eingefügte Zeilen, aktualisierte Zeilen und gelöschte Zeilen	Lesen	ReplicationTask*		
DisassociateExtensionPack	Gewährt die Berechtigung zum Trennen eines Erweiterungspakets	Schreiben	MigrationProject*		
ExportMetadataModelAssessment	Gewährt die Berechtigung zum Löschen der angegebenen Metadatenmodellbewertung	Schreiben	MigrationProject		
GetMetadataModel	Gewährt die Berechtigung zum Auflisten aller AWS DMS-Attribute für ein Metadatenmodell. Hinweis: Obwohl diese Aktion erfordert StartMetadataModelImport, autorisiert letzteres derzeit nicht den beschriebenen Schemakonvertierungsvorgang	Lesen	MigrationProject		dms:StartMetadataModelImport

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ImportCertificate	Gewährt die Berechtigung zum Upload des angegebenen Zertifikats	Schreiben		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
ListDataProviders	Gewährt die Berechtigung zum Auflisten der AWS DMS-Attribute für einen Datenanbieter	Lesen	DataProvider		dms:DescribeDataProviders
ListExtensionPacks	Gewährt die Berechtigung zum Auflisten der AWS DMS-Attribute für ein Erweiterungspaket	Lesen	MigrationProject		dms:DescribeExtensionPackAssociations
ListInstanceProfiles	Gewährt die Berechtigung zum Auflisten der AWS DMS-Attribute für ein Instance-Profil	Lesen	InstanceProfile		dms:DescribeInstanceProfiles

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListMetadataModelAssessmentActionItems	Gewährt die Berechtigung zum Auflisten der AWS DMS-Attribute für eine Metadaten modell-Bewertungsaktion. Hinweis: Obwohl diese Aktion erfordert StartMetadataModelImport, autorisiert letzteres derzeit nicht den beschriebenen Schemakonvertierungsvorgang	Lesen	Migration Project		dms:StartMetadataModelImport
ListMetadataModelAssessments	Gewährt die Berechtigung zum Auflisten der AWS DMS-Attribute für Metadaten modellbewertungen	Lesen	Migration Project		dms:DescribeMetadataModelAssessments
ListMetadataModelConversions	Gewährt die Berechtigung zum Auflisten der AWS DMS-Attribute für eine Metadaten modellkonvertierung	Lesen	Migration Project		dms:DescribeMetadataModelConversions
ListMetadataModelExports	Gewährt die Berechtigung zum Auflisten der AWS DMS-Attribute für einen Metadaten modellexport	Lesen	Migration Project		dms:DescribeMetadataModelExportsAsScript dms:DescribeMetadataModelExportsToTarget

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListMigrationProjects	Gewährt die Berechtigung zum Auflisten der AWS DMS-Attribute für ein Migrationsprojekt. Hinweis: Obwohl diese Aktion DescribeMigrationProjects und erfordert DescribeConversionConfiguration, autorisieren beide erforderlichen Aktionen derzeit nicht den beschriebenen Schemakonvertierungsvorgang	Lesen	DataProvider		dms:DescribeConversionConfiguration dms:DescribeMigrationProjects
			InstanceProfile		
			MigrationProject		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten aller Tags für eine -DMS AWS -Ressource	Lesen	Certificate		
			DataMigration		
			DataProvider		
			Endpoint		
			EventSubscription		
			InstanceProfile		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			Migration Project		
			ReplicationConfig		
			ReplicationInstance		
			ReplicationSubnetGroup		
			ReplicationTask		
ModifyConversionConfiguration [nur Berechtigung]	Gewährt die Berechtigung, eine Konvertierungskonfiguration zu aktualisieren. Hinweis: Diese Aktion sollte zusammen mit hinzugefügt werden UpdateConversionConfiguration, autorisiert derzeit jedoch nicht den beschriebenen Schemakonvertierungsvorgang	Schreiben	Migration Project*		dms:UpdateConversionConfiguration
ModifyDataMigration	Gewährt die Berechtigung zum Ändern der angegebenen Datenbankmigration	Schreiben	DataMigration*		iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyDataProvider [nur Berechtigung]	Gewährt die Berechtigung, den angegebenen Datenanbieter zu bearbeiten. Hinweis: Diese Aktion sollte zusammen mit hinzugefügt werden UpdateDataProvider, autorisiert derzeit jedoch nicht den beschriebenen Schemakonvertierungsvorgang	Schreiben	DataProvider*		dms:UpdateDataProvider iam:PassRole
ModifyEndpoint	Gewährt die Berechtigung zum Ändern des angegebenen Endpunkts	Schreiben	Endpoint* Certificate		iam:PassRole
ModifyEventSubscription	Gewährt die Berechtigung zum Ändern eines bestehenden AWS DMS-Ereignisbenachrichtigungsabonnements	Schreiben			
ModifyFleetAdvisorCollector [nur Berechtigung]	Gewährt die Berechtigung zum Ändern des Namens und der Beschreibung des angegebenen Fleet-Advisor-Collector	Schreiben			
ModifyFleetAdvisorCollectorStatuses [nur Berechtigung]	Gewährt die Berechtigung zum Ändern des Status des angegebenen Fleet-Advisor-Collector	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyInstanceProfile [nur Berechtigung]	Gewährt die Berechtigung, das angegebene Instance-Profil zu bearbeiten. Hinweis: Diese Aktion sollte zusammen mit hinzugefügt werden UpdateInstanceProfile, autorisiert derzeit jedoch nicht den beschriebenen Schemakonvertierungsvorgang	Schreiben	InstanceProfile*		dms:UpdateInstanceProfile iam:PassRole
ModifyMigrationProject [nur Berechtigung]	Gewährt die Berechtigung, das angegebene Migrationsprojekt zu bearbeiten. Hinweis: Diese Aktion sollte zusammen mit hinzugefügt werden UpdateMigrationProject, autorisiert derzeit jedoch nicht den beschriebenen Schemakonvertierungsvorgang	Schreiben	MigrationProject*		dms:UpdateMigrationProject iam:PassRole
ModifyReplicationConfig	Gewährt die Berechtigung zum Ändern der angegebenen Replikationskonfiguration	Schreiben	ReplicationConfig*		
ModifyReplicationInstance	Gewährt die Berechtigung, die Replikations-Instance zu ändern, um neue Einstellungen anzuwenden	Write	ReplicationInstance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyReplicationSubnetGroup	Gewährt die Berechtigung zum Ändern der Einstellungen für die angegebene Replikationssubnetzgruppe	Write			
ModifyReplicationTask	Gewährt die Berechtigung zum Ändern der angegebenen Replikationsaufgabe	Write	ReplicationTask*		
MoveReplicationTask	Gewährt die Berechtigung zum Verschieben der angegebenen Replikationsaufgabe auf eine andere Replikations-Instance	Write	ReplicationInstance*		
			ReplicationTask*		
RebootReplicationInstance	Gewährt die Berechtigung zum Neustart einer Replikations-Instance. Ein Neustart führt zu einem kurzzeitigen Ausfall, bis die Replikations-Instance wieder verfügbar ist.	Write	ReplicationInstance*		
RefreshSchemas	Gewährt die Berechtigung, das Schema für den angegebenen Endpunkt zu füllen	Schreiben	Endpoint*		
			ReplicationInstance*		
ReloadReplicationTables	Gewährt die Berechtigung zum Neuladen der Zieldatenbanktabelle mit der Quelle für eine Replikation	Schreiben	ReplicationConfig*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ReloadTables	Gewährt die Berechtigung, die Zieldatenbanktabelle mit den Quelldaten neu zu laden	Write	ReplicationTask*		
RemoveTagsFromResource	Gewährt die Berechtigung zum Entfernen von Metadaten-Tags aus einer DMS-Ressource	Tagging	Certificate		
			DataMigration		
			DataProvider		
			Endpoint		
			EventSubscription		
			InstanceProfile		
			MigrationProject		
			ReplicationConfig		
			ReplicationInstance		
			ReplicationSubnetGroup		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			ReplicationTask		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
RunFleetAdvisorLsaAnalysis	Gewährt die Berechtigung, für jeden Fleet-Advisor-Collector in Ihrem Konto eine LSA (large-scale assessment)-Analyse durchzuführen	Schreiben			
StartDataMigration	Gewährt die Berechtigung zum Starten der angegebenen Datenbankmigration	Schreiben	DataMigration*		
StartExtensionPackAssociation [nur Berechtigung]	Gewährt die Berechtigung, ein Erweiterungspaket zuzuordnen. Hinweis: Diese Aktion sollte zusammen mit hinzugefügt werden AssociateExtensionPack, autorisiert derzeit jedoch nicht den beschriebenen Schemakonvertierungsvorgang	Schreiben	MigrationProject*		dms:AssociateExtensionPack

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartMetadataModelAssessment	Gewährt die Berechtigung zum Starten einer neuen Bewertung des Metadatenmodells	Schreiben	Migration Project*		
StartMetadataModelConversion	Gewährt die Berechtigung zum Starten einer neuen Konvertierung des Metadatenmodells	Schreiben	Migration Project*		
StartMetadataModelExportAsScript [nur Berechtigung]	Gewährt die Berechtigung, einen neuen Export eines Metadatenmodells als Skript zu starten. Hinweis: Diese Aktion sollte zusammen mit hinzugefügt werden StartMetadataModelExportAsScripts, autorisiert derzeit jedoch nicht den beschriebenen Schemakonvertierungsvorgang	Schreiben	Migration Project*		dms:StartMetadataModelExportAsScripts
StartMetadataModelExportAsScripts	Gewährt die Berechtigung zum Starten eines neuen Exportes eines Metadatenmodells als Skript	Schreiben	Migration Project*		dms:StartMetadataModelExportAsScript
StartMetadataModelExportToTarget	Gewährt die Berechtigung zum Starten eines neuen Exportes des Metadatenmodells an das Ziel	Schreiben	Migration Project*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartMetadataModelImport	Gewährt die Berechtigung zum Starten eines neuen Imports eines Metadatenmodells	Schreiben	MigrationProject*		
StartRecommendations	Gewährt die Berechtigung zum Starten der Analyse Ihrer Quelldatenbank, um Empfehlungen für Ziel-Engines abzugeben	Schreiben			
StartReplication	Gewährt die Berechtigung zum Starten einer Replikation	Schreiben	ReplicationConfig*		
StartReplicationTask	Gewährt die Berechtigung zum Starten der Replikationsaufgabe	Write	ReplicationTask*		
StartReplicationTaskAssessment	Gewährt die Berechtigung zum Starten der Replikationsaufgabenbewertung für nicht unterstützte Datentypen in der Quelldatenbank	Write	ReplicationTask*		
StartReplicationTaskAssessmentRun	Gewährt die Berechtigung, einen neuen Bewertungslauf vor der Migration für eine oder mehrere Einzelbewertungen einer Migrationsaufgabe zu starten	Schreiben	ReplicationTask*		iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopDataMigration	Gewährt die Berechtigung zum Stoppen der Datenbankmigration	Schreiben	DataMigration*		
StopReplication	Gewährt die Berechtigung zum Stoppen einer Replikation	Schreiben	ReplicationConfig*		
StopReplicationTask	Gewährt die Berechtigung zum Beenden der Replikationsaufgabe	Write	ReplicationTask*		
TestConnection	Gewährt die Berechtigung zum Testen der Verbindung zwischen der Replikations-Instance und dem Endpunkt	Lesen	Endpoint*		
			ReplicationInstance*		
UpdateConversionConfiguration	Gewährt die Berechtigung zum Aktualisieren einer Konvertierungskonfiguration	Schreiben	MigrationProject*		dms:ModifyConversionConfiguration
UpdateDataProvider	Gewährt die Berechtigung zum Aktualisieren des angegebenen Datenanbieters	Schreiben	DataProvider*		dms:ModifyDataProvider
UpdateInstanceProfile	Gewährt die Berechtigung zum Aktualisieren des angegebenen Instance-Profils	Schreiben	InstanceProfile*		dms:ModifyInstanceProfile
UpdateMigrationProject	Gewährt die Berechtigung zum Aktualisieren des angegebenen Migrationsprojekts	Schreiben	MigrationProject*		dms:ModifyMigrationProject

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateSubscriptionsToEventBridge	Gewährt die Berechtigung, DMS-Abonnements zu Eventbridge zu migrieren	Schreiben			
UploadFileMetadataList [nur Berechtigung]	Gewährt die Berechtigung, Dateien in Ihren Amazon-S3-Bucket hochzuladen	Schreiben			

Von AWS Database Migration Service definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Certificate	`arn:${Partition}:dms:${Region}:${Account}:cert:*`	aws:ResourceTag/${TagKey} dms:cert-tag/${TagKey}
DataProvider	`arn:${Partition}:dms:${Region}:${Account}:data-provider:*`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
		dms:data-provider-tag/${TagKey}
DataMigration	arn:${Partition}:dms:${Region}:${Account}:data-migration:*	aws:ResourceTag/${TagKey} dms:data-migration-tag/${TagKey}
Endpoint	arn:${Partition}:dms:${Region}:${Account}:endpoint:*	aws:ResourceTag/${TagKey} dms:endpoint-tag/${TagKey}
EventSubscription	arn:${Partition}:dms:${Region}:${Account}:es:*	aws:ResourceTag/${TagKey} dms:es-tag/${TagKey}
InstanceProfile	arn:${Partition}:dms:${Region}:${Account}:instance-profile:*	aws:ResourceTag/${TagKey} dms:instance-profile-tag/${TagKey}
MigrationProject	arn:${Partition}:dms:${Region}:${Account}:migration-project:*	aws:ResourceTag/${TagKey} dms:migration-project-tag/${TagKey}
ReplicationConfig	arn:${Partition}:dms:${Region}:${Account}:replication-config:*	aws:ResourceTag/${TagKey} dms:replication-config-tag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
ReplicationInstance	arn:${Partition}:dms:${Region}:${Account}:rep:*	aws:ResourceTag/${TagKey} dms:rep-tag/${TagKey}
ReplicationSubnetGroup	arn:${Partition}:dms:${Region}:${Account}:subgrp:*	aws:ResourceTag/${TagKey} dms:subgrp-tag/${TagKey}
ReplicationTask	arn:${Partition}:dms:${Region}:${Account}:task:*	aws:ResourceTag/${TagKey} dms:task-tag/${TagKey}
ReplicationTaskAssessmentRun	arn:${Partition}:dms:${Region}:${Account}:assessment-run:*	
ReplicationTaskIndividualAssessment	arn:${Partition}:dms:${Region}:${Account}:individual-assessment:*	

Bedingungsschlüssel für AWS Database Migration Service

AWS Database Migration Service definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüsselwertpaaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString
dms:cert-tag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung für ein Zertifikat	String
dms:data-migration-tag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung für DataMigration	String
dms:data-provider-tag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung für DataProvider	String
dms:endpoint-tag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung für einen Endpunkt	String
dms:es-tag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung für EventSubscription	String
dms:instance-profile-tag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung für InstanceProfile	String

Bedingungsschlüssel	Beschreibung	Typ
dms:migration-project-tag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung für Migration Project	String
dms:rep-tag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung für ReplicationInstance	String
dms:replication-config-tag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung für ReplicationConfig	String
dms:req-tag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der angegebenen Anforderung	String
dms:subgrp-tag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung für ReplicationSubnetGroup	String
dms:task-tag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung für ReplicationTask	String

Aktionen, Ressourcen und Bedingungsschlüssel für Database Query Metadata Service

Database Query Metadata Service (Servicepräfix: `dbqms`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.

- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Database Query Metadata Service definierte Aktionen
- Von Database Query Metadata Service definierte Ressourcentypen
- Bedingungsschlüssel für Database Query Metadata Service

Von Database Query Metadata Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateFavoriteQuery	Gewährt die Berechtigung zum Erstellen einer neuen bevorzugten Abfrage	Write			
CreateQueryHistory	Gewährt die Berechtigung zum Hinzufügen einer Abfrage zum Verlauf	Write			
CreateTab	Gewährt die Berechtigung zum Erstellen einer neuen Abfrage-Registerkarte	Write			
DeleteFavoriteQueries	Gewährt die Berechtigung zum Löschen gespeicherter Abfragen	Write			
DeleteQueryHistory	Gewährt die Berechtigung zum Löschen einer Verlaufsabfrage	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteTab	Gewährt die Berechtigung zum Löschen der Registerkarte „Abfrage“	Write			
DescribeFavoriteQueries	Gewährt die Berechtigung zum Auflisten gespeicherter Abfragen und zugehöriger Metadaten	List			
DescribeQueryHistory	Gewährt die Berechtigung zum Auflisten des Verlaufs der ausgeführten Abfragen	List			
DescribeTabs	Gewährt die Berechtigung zum Auflisten von Abfrage-Registerkarten und zugehörigen Metadaten	List			
GetQueryString	Gewährt die Berechtigung zum Abrufen der bevorzugten oder Verlaufsabfragezeichenfolge nach ID	Read			
UpdateFavoriteQuery	Gewährt die Berechtigung zum Aktualisieren einer gespeicherten Abfragen und Beschreibung	Write			
UpdateQueryHistory	Gewährt die Berechtigung zum Aktualisieren des Abfrageverlaufs	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateTab	Gewährt die Berechtigung zum Aktualisieren der Registerkarte „Abfrage“	Write			

Von Database Query Metadata Service definierte Ressourcentypen

Database Query Metadata Service unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf den Database Query Metadata Service zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für Database Query Metadata Service

DBQMS hat keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS DataSync

AWS DataSync (Servicepräfix: `datasync`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS DataSync definierte Aktionen
- Von AWS DataSync definierte Ressourcentypen
- Bedingungsschlüssel für AWS DataSync

Von AWS DataSync definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddStorageSystem	Gewährt die Berechtigung zum Erstellen eines Speichersystems	Schreiben	agent*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CancelTaskExecution	Gewährt die Berechtigung zum Abbrechen der Ausführung einer Synchronisationsaufgabe	Write	taskexecution*		
				aws:ResourceTag/${TagKey}	
CreateAgent	Gewährt die Berechtigung zur Aktivierung eines Agenten, den Sie auf Ihrem Host bereitgestellt haben	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationAzureBlob	Erteilt die Berechtigung, einen Endpunkt für einen Microsoft Azure Blob Storage-Container zu erstellen	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateLocationEfs	Gewährt die Berechtigung zum Erstellen eines Endpunkts für ein Amazon-EFS-Dateisystem	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationFsxLustre	Gewährt die Berechtigung zum Erstellen eines Endpunkts für Amazon Fsx for Lustre	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationFsxOntap	Erteilung der Berechtigung zum Erstellen eines Endpunkts für Amazon FSx für ONTAP	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationFsxOpenZfs	Gewährt die Berechtigung zum Erstellen eines Endpunkts für Amazon FSx for OpenZFS	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationFsxWindows	Gewährt die Berechtigung zum Erstellen eines Endpunkts für ein Amazon-FSx-Windows-File-Server-Dateisystem	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateLocationHdfs	Gewährt die Berechtigung zum Erstellen eines Endpunkts für ein Amazon-HDFS	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationNfs	Gewährt die Berechtigung zum Erstellen eines Endpunkts für ein NFS-Dateisystem	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationObjectStorage	Gewährt die Berechtigung zum Erstellen eines Endpunkts für einen selbstverwalteten Objektspeicher-Bucket	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationS3	Gewährt die Berechtigung zum Erstellen eines Endpunkts für einen Amazon-S3-Bucket	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationSmb	Gewährt die Berechtigung zum Erstellen eines Endpunkts für ein SMB-Dateisystem	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTask	Gewährt die Berechtigung zum Erstellen einer Synchronisierungsaufgabe	Schreiben	location*		
			agent		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAgent	Gewährt die Berechtigung zum Löschen eines Agenten	Write	agent*		
DeleteLocation	Gewährt die Berechtigung zum Löschen eines von AWS DataSync verwendeten Speicherorts	Write	location*		
DeleteTask	Gewährt die Berechtigung zum Löschen einer Synchronisierungsaufgabe	Write	task*		
DescribeAgent	Gewährt die Berechtigung zum Anzeigen von Metadaten, wie Name, Netzwerkschnittstellen, sowie den Status (d h., ob der Agent ausgeführt wird oder nicht) eines Synchronisierungsagenten	Lesen	agent*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDiscoveryJob	Gewährt die Berechtigung zum Beschreiben der Metadaten über eine Aufgabe zur Erkennung	Lesen	discovery job*		
DescribeLocationAzureBlob	Erteilt die Berechtigung zum Anzeigen von Metadaten, wie den Pfadinformationen, über einen SMB-Synchronisierungsspeicherort	Lesen	location*		
DescribeLocationEfs	Gewährt die Berechtigung zum Anzeigen von Metadaten, z. B. die Pfadinformationen zu einem Amazon-EFS-Synchronisierungsspeicherort	Lesen	location*		
DescribeLocationFsxLustre	Gewährt die Berechtigung zum Anzeigen von Metadaten, wie den Pfadinformationen zu einem Synchronisierungsspeicherort für Amazon FSx for Lustre	Lesen	location*		
DescribeLocationFsxOntap	Erteilung der Berechtigung zum Anzeigen von Metadaten, z. B. der Pfadinformationen zu einem Amazon FSx für ONTAP-Synchronisierungsort	Lesen	location*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeLocationFsxOpenZfs	Gewährt die Berechtigung zum Anzeigen von Metadaten, wie den Pfadinformationen zu einem Synchronisierungsspeicherort für Amazon FSx OpenZFS	Lesen	location*		
DescribeLocationFsxWindows	Gewährt die Berechtigung zum Anzeigen von Metadaten wie die Pfadinformationen zu einem Amazon-FSx-Windows-Synchronisierungsspeicherort	Lesen	location*		
DescribeLocationHdfs	Gewährt die Berechtigung zum Anzeigen von Metadaten, wie den Pfadinformationen zu einem Synchronisierungsspeicherort für ein Amazon-HDFS	Lesen	location*		
DescribeLocationNfs	Gewährt die Berechtigung zum Anzeigen von Metadaten, wie den Pfadinformationen, zu einem NFS-Synchronisierungsspeicherort	Read	location*		
DescribeLocationObjectStorage	Gewährt die Berechtigung zum Anzeigen von Metadaten zum Speicherort eines selbstverwalteten Objektspeicherservers	Read	location*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeLocationS3	Gewährt die Berechtigung zum Anzeigen von Metadaten wie Bucket-Namen über einen Amazon-S3-Bucket-Synchronisierungsspeicherort	Read	location*		
DescribeLocationSmb	Gewährt die Berechtigung zum Anzeigen von Metadaten, wie den Pfadinformationen, über einen SMB-Synchronisierungsspeicherort	Lesen	location*		
DescribeStorageSystem	Gewährt die Berechtigung zum Anzeigen von Metadaten über ein Speichersystem	Lesen	storagesystem*		
DescribeStorageSystemResourceMetrics	Gewährt die Berechtigung zum Beschreiben von Ressourcenkennzahlen, die im Rahmen einer Datenerkennungsaufgabe erfasst wurden	Auflisten	discoveryjob*		
DescribeStorageSystemResources	Gewährt die Berechtigung zum Beschreiben von Ressourcen, die im Rahmen einer Erkennungsaufgabe erfasst wurden	Auflisten	discoveryjob*		
DescribeTask	Gewährt die Berechtigung zum Anzeigen von Metadaten zu einer Synchronisierungsaufgabe	Read	task*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeTaskExecution	Gewährt die Berechtigung zum Anzeigen von Metadaten zu einer durchgeführten Synchronisierungsaufgabe	Lesen	taskexecution*		
				aws:ResourceTag/${TagKey}	
GenerateRecommendations	Gewährt die Berechtigung, Empfehlungen für eine Ressource zu generieren, die im Rahmen einer Erkennungsaufgabe identifiziert wurde	Schreiben	discoveryjob*		
ListAgents	Gewährt die Berechtigung zum Auflisten von Agenten, die einem AWS-Konto in einer in der Anfrage angegebenen Region gehören	Auflisten			
ListDiscoveryJobs	Gewährt die Berechtigung zum Auflisten von Erkennungsaufgaben	Auflisten			
ListLocations	Gewährt die Berechtigung, Quell- und Zielsynchronisierungsspeicherorte aufzulisten	Auflisten			
ListStorageSystems	Gewährt die Berechtigung zum Auflisten von Speichersystemen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung, die Tags aufzulisten, die der angegebenen Ressource hinzugefügt wurden	Read	agent		
			discoveryjob		
			location		
			storagesystem		
			task		
			taskexecution		
ListTaskExecutions	Gewährt die Berechtigung zum Auflisten ausgeführter Synchronisierungsaufgaben	List		aws:ResourceTag/${TagKey}	
ListTasks	Gewährt die Berechtigung zum Auflisten aller Synchronisierungsaufgaben	Auflisten			
RemoveStorageSystem	Gewährt die Berechtigung zum Löschen eines Speichersystems	Schreiben	storagesystem*		
StartDiscoveryJob	Gewährt die Berechtigung zum Starten einer Erkennungsaufgabe für ein Speichersystem	Schreiben	storagesystem*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartTaskExecution	Gewährt die Berechtigung, einen bestimmten Aufruf einer Synchronisationsaufgabe zu starten	Schreiben	task*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
StopDiscoveryJob	Gewährt die Berechtigung zum Stoppen einer Erkennungsaufgabe	Schreiben	discoveryjob*		
TagResource	Gewährt die Berechtigung, ein Schlüssel-Wert-Paar auf eine AWS-Ressource anzuwenden	Markierung	agent		
			discoveryjob		
			location		
			storagesystem		
			task		
			taskexecution		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen eines oder mehrerer Tags aus der angegebenen Ressource	Markierung	agent		
			discoveryjob		
			location		
			storagesystem		
			task		
			taskexecution		
				aws:TagKeys	
UpdateAgent	Gewährt die Berechtigung, den Namen eines Agenten zu aktualisieren	Schreiben	agent*		
UpdateDiscoveryJob	Gewährt die Berechtigung zum Aktualisieren eines Erkennungsauftrags	Schreiben	discoveryjob*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateLocationAzureBlob	Erteilt die Berechtigung zum Aktualisieren eines Azure Blob Storage-Synchronisierungsspeicherorts	Schreiben	location*		
UpdateLocationHdfs	Gewährt die Berechtigung zum Aktualisieren eines HDFS-Synchronisierungsspeicherorts	Schreiben	location*		
UpdateLocationNfs	Gewährt die Berechtigung zum Aktualisieren eines NFS-Synchronisierungsspeicherorts	Schreiben	location*		
UpdateLocationObjectStorage	Gewährt die Berechtigung zum Anzeigen von Metadaten zum Speicherort eines selbstverwalteten Objektspeicherservers	Schreiben	location*		
UpdateLocationSmb	Gewährt die Berechtigung zum Aktualisieren eines SMB-Synchronisierungsorts	Schreiben	location*		
UpdateStorageSystem	Gewährt die Berechtigung zum Aktualisieren eines Speichersystems	Schreiben	storagesystem*		
UpdateTask	Gewährt die Berechtigung zum Aktualisieren von Metadaten, die mit einer Synchronisierungsaufgabe verknüpft sind	Write	task*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateTaskExecution	Gewährt die Berechtigung zum Aktualisieren der Ausführung einer Synchronisierungsaufgabe	Schreiben	taskexecution*		
				aws:ResourceTag/${TagKey}	

Von AWS DataSync definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
agent	`arn:${Partition}:datasync:${Region}:${AccountId}:agent/${AgentId}`	aws:ResourceTag/${TagKey}
location	`arn:${Partition}:datasync:${Region}:${AccountId}:location/${LocationId}`	aws:ResourceTag/${TagKey}
task	`arn:${Partition}:datasync:${Region}:${AccountId}:task/${TaskId}`	aws:ResourceTag/${TagKey}
taskexecution	`arn:${Partition}:datasync:${Region}:${AccountId}:task/${TaskId}/execution/${ExecutionId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
storagesystem	`arn:${Partition}:datasync:${Region}:${AccountId}:system/${StorageSystemId}`	aws:ResourceTag/${TagKey}
discoveryjob	`arn:${Partition}:datasync:${Region}:${AccountId}:system/${StorageSystemId}/job/${DiscoveryJobId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS DataSync

AWS DataSync definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tag-Schlüssel-Wert-Paare in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach den Schlüssel-Wert-Paaren der Tags, die der Ressource zugeordnet sind	Zeichenfolge
aws:TagKeys	Filtert Aktionen nach den Tag-Schlüsseln in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon DataZone

Amazon DataZone (Service-Präfix:`datazone`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon definierte Aktionen DataZone

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptPredictions	Gewährt die Berechtigung zum Annehmen einer Vorhersage	Schreiben			
AcceptSubscriptionRequest	Gewährt die Berechtigung zum Genehmigen einer Abonnementanforderung nach einem Datenbestand	Schreiben			
AddPolicyGrant [nur Berechtigung]	Erteilt die Erlaubnis, einen Policy-Zuschuss hinzuzufügen	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelMetadataGenerationRun	Erteilt die Erlaubnis, den Lauf der Metadaten-Generierung abzubrechen	Schreiben			
CancelSubscription	Gewährt die Berechtigung zum Widerrufen oder Kündigen eines genehmigten Abonnements eines Datenbestands	Schreiben			
CreateAsset	Gewährt die Berechtigung zum Erstellen eines Datenbestands	Schreiben			
CreateAssetRevision	Gewährt die Berechtigung zum Erstellen einer neuen Version eines Datenbestands	Schreiben			
CreateAssetType	Gewährt die Berechtigung zum Erstellen eines Bestandstypen	Schreiben			
CreateDataSource	Erteilt die Erlaubnis, ein neues zu erstellen DataSource	Schreiben			
CreateDomain	Erteilt die Genehmigung zur Bereitstellung einer Domain, bei der es sich um eine Entität der obersten Ebene handelt, die andere DataZone Amazon-Ressourcen enthält	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateEnvironment	Gewährt die Berechtigung zum Erstellen einer Sammlung konfigurierter Ressourcen, die zum Veröffentlichen und Abonnieren von Daten verwendet werden	Schreiben			
CreateEnvironmentBlueprint [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer benutzerdefinierten Umgebungsvorlage, mit der Benutzer Umgebungen zu ihrem Projekt hinzufügen können	Schreiben			
CreateEnvironmentProfile	Gewährt die Berechtigung zum Erstellen einer Vorlage, die zur Erstellung einer Umgebung verwendet werden kann	Schreiben			
CreateFormType	Gewährt die Berechtigung zum Erstellen eines Formulartyps oder einer neuen Version davon	Schreiben			
CreateGlossary	Gewährt die Berechtigung zum Erstellen eines Geschäftsglossars	Schreiben			
CreateGlossaryTerm	Gewährt die Berechtigung zum Erstellen eines Glossarbegriffs	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateGroupProfile	Erteilt die Berechtigung, ein DataZone Gruppenprofil für eine IAM Identity Center-Gruppe zu erstellen	Schreiben			
CreateListingChangeSet	Gewährt die Berechtigung zum Erstellen eines Auflistungsänderungssatzes	Schreiben			
CreateProject	Gewährt die Berechtigung zum Erstellen eines Projekts, damit Ihr Team Daten veröffentlichen und abonnieren kann	Schreiben			
CreateProjectMembership	Gewährt die Berechtigung zum Hinzufügen eines Benutzers zu einem Projekt	Schreiben			
CreateSubscriptionGrant	Gewährt die Berechtigung zum Erstellen einer Berechtigung für ein genehmigtes Abonnement oder ein Abonnementziel	Schreiben			
CreateSubscriptionRequest	Gewährt die Berechtigung zum Erstellen einer Abonnementanforderung nach einem Datenbestand	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSubscriptionTarget	Gewährt die Berechtigung zum Erstellen eines Abonnementziels für eine Umgebung in einem Projekt	Schreiben			
CreateUserProfile	Gewährt die Berechtigung zum Erstellen eines Benutzerprofils für einen vorhandenen Benutzer im IAM Identity Center des Kunden	Schreiben			
DeleteAsset	Gewährt die Berechtigung zum Löschen einer Komponente	Schreiben			
DeleteAssetType	Gewährt die Berechtigung zum Löschen eines Bestandstyps	Schreiben			
DeleteDataSource	Erteilt die Erlaubnis, bestehende zu aktualisieren DataSource	Schreiben			
DeleteDomain	Gewährt die Berechtigung zum Löschen einer bereitgestellten Domain	Schreiben	domain*		
DeleteDomainSharingPolicy [nur Berechtigung]	Erteilt die Berechtigung zum Löschen einer Ressourcenrichtlinie für eine DataZone Domäne	Berechtigungsverwaltung			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteEnvironment	Gewährt die Berechtigung zum Löschen einer Umgebung	Schreiben			
DeleteEnvironmentBlueprint [nur Berechtigung]	Gewährt die Berechtigung zum Löschen einer Umgebungsvorlage	Schreiben			
DeleteEnvironmentBlueprintConfiguration	Gewährt die Berechtigung zum Löschen einer Umgebungsvorlagenkonfiguration	Schreiben			
DeleteEnvironmentProfile	Gewährt die Berechtigung zum Löschen eines Umgebungsprofils	Schreiben			
DeleteFormType	Gewährt die Berechtigung zum Löschen eines Formulartyps	Schreiben			
DeleteGlossary	Gewährt die Berechtigung zum Löschen eines Geschäftsglossars	Schreiben			
DeleteGlossaryTerm	Gewährt die Berechtigung zum Löschen eines Glossarbegriffs	Schreiben			
DeleteListing	Gewährt die Berechtigung zum Löschen einer Auflistung	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteProject	Gewährt die Berechtigung zum Löschen eines Projekts, das Ihrem Team ermöglicht, Daten zu veröffentlichen und zu abonnieren	Schreiben			
DeleteProjectMembership	Gewährt die Berechtigung zum Entfernen eines Benutzers aus einem Projekt	Schreiben			
DeleteSubscriptionGrant	Gewährt die Berechtigung zum Löschen einer Berechtigung für ein genehmigtes Abonnement oder ein Abonnementziel	Schreiben			
DeleteSubscriptionRequest	Gewährt die Berechtigung zum Löschen einer ausstehenden Abonnementanforderung nach einem Datenbestand	Schreiben			
DeleteSubscriptionTarget	Gewährt die Berechtigung zum Löschen eines Abonnementziels aus einer Umgebung im Projekt	Schreiben			
DeleteTimeSeriesDataPoints	Erteilt die Erlaubnis, bestehende zu löschen TimeSeriesDataPoints	Schreiben			
GetAsset	Gewährt die Berechtigung zum Abrufen eines Bestands	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAssetType	Gewährt die Berechtigung zum Abrufen eines Bestandstyps	Lesen			
GetDataSource	Erteilt die Erlaubnis, ein DataSource in Amazon vorhandenes Objekt DataZone anhand seiner Kennung abzurufen	Lesen			
GetDataSourceRun	Erteilt die Erlaubnis, den DataSource ausgeführten Job in Amazon DataZone mithilfe seiner Kennung abzurufen	Lesen			
GetDomain	Gewährt die Berechtigung zum Abrufen von Informationen über die Domain	Lesen	domain*		
GetDomainSharingPolicy [nur Berechtigung]	Erteilt die Erlaubnis zum Abrufen einer Ressourcenrichtlinie für eine DataZone Domain	Lesen			
GetEnvironment	Gewährt die Berechtigung zum Abrufen von Details zu einer Umgebung	Lesen			
GetEnvironmentActionLink [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen des Umgebungsaktionslinks	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetEnvironmentBlueprint	Gewährt die Berechtigung zum Abrufen von Details zu einer Umgebungsvorlage	Lesen			
GetEnvironmentBlueprintConfiguration	Gewährt die Berechtigung zum Abrufen einer Umgebungsvorlagenkonfiguration	Lesen			
GetEnvironmentCredentials	Gewährt die Berechtigung zum Abrufen kurzfristiger Anmeldeinformationen, die die Benutzerrolle „Umgebung“ annehmen	Lesen			
GetEnvironmentProfile	Gewährt die Berechtigung zum Abrufen von Details zu einem Umgebungsprofil	Lesen			
GetFormType	Gewährt die Berechtigung zum Abrufen eines Formulartyps	Lesen			
GetGlossary	Gewährt die Berechtigung zum Abrufen eines Geschäftsglossars	Lesen			
GetGlossaryTerm	Gewährt die Berechtigung zum Abrufen eines Glossarbegriffs	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetGroupProfile	Erteilt die Berechtigung zum Abrufen eines vorhandenen DataZone Gruppenprofils	Lesen			
GetIamPortalLoginUrl	Erteilt einem IAM-Prinzipal die Erlaubnis, sich beim DataZone Portal anzumelden	Berechtigungsverwaltung			
GetListing	Gewährt die Berechtigung zum Abrufen einer Auflistung	Lesen			
GetMetadataGenerationRun	Gewährt die Berechtigung zum Abrufen des Metadatengenerierungslaufs	Lesen			
GetProject	Gewährt die Berechtigung zum Abrufen von Projektdetails	Lesen			
GetSubscription	Gewährt die Berechtigung zum Abrufen eines Abonnements	Lesen			
GetSubscriptionEligibility [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen der Abonnementberechtigung	Lesen			
GetSubscriptionGrant	Gewährt die Berechtigung zum Abrufen einer Abonnementgewährung	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetSubscriptionRequestDetails	Gewährt die Berechtigung zum Ablehnen einer Abonnementanforderung nach einem Datenbestand	Lesen			
GetSubscriptionTarget	Gewährt die Berechtigung zum Abrufen eines Abonnementziels	Lesen			
GetTimeSeriesDataPoint	Erteilt die Erlaubnis, ein TimeSeriesDataPoints in Amazon vorhandenes Objekt DataZone anhand seiner Kennung abzurufen	Lesen			
GetUserProfile	Erteilt die Erlaubnis, ein Benutzerprofil für einen vorhandenen Benutzer in der DataZone Domain abzurufen	Lesen			
ListAccountEnvironments	Erteilt die Berechtigung, Umgebungen in allen Domänen eines AWS Kontos aufzulisten	Auflisten			
ListAssetRevisions	Gewährt die Berechtigung zum Auflisten der Versionen eines Bestands	Auflisten			
ListDataSourceRunActivities	Erteilt die Erlaubnis, die Aktivitäten von Run-Jobs auf Asset aufzulisten DataSource	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDataSourceRuns	Erteilt die Berechtigung, ausgeführte DataSource Jobs aufzulisten	Auflisten			
ListDataSources	Erteilt die Erlaubnis, bestehende aufzulisten DataSources	Auflisten			
ListDomains	Gewährt die Berechtigung zum Abrufen aller Domains	Auflisten			
ListEnvironmentBlueprintConfigurationSummaries [nur Berechtigung]	Erteilt die Berechtigung, Zusammenfassungen der Umgebungs-Blueprint-Konfigurationen aufzulisten	Auflisten			
ListEnvironmentBlueprintConfigurations	Gewährt die Berechtigung zum Auflisten von Vorlagenkonfigurationen	Auflisten			
ListEnvironmentBlueprints	Gewährt die Berechtigung zum Auflisten der Domain für Umgebungsvorlagen	Auflisten			
ListEnvironmentProfiles	Gewährt die Berechtigung zum Auflisten der Domain für Umgebungsprofile	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListEnvironments	Gewährt die Berechtigung zum Anzeigen von Umgebungen in der Domain	Auflisten			
ListGroupsForUser	Erteilt die Berechtigung, alle DataZone Gruppenprofile aufzulisten, in denen das DataZone Benutzerprofil Mitglied ist	Auflisten			
ListMetadataGenerationRuns	Gewährt die Berechtigung zum Auflisten von Metadatengenerierungsläufen	Auflisten			
ListNotifications	Gewährt die Berechtigung zum Auflisten von Benachrichtigungen und Ereignissen für den DataZone-Benutzer	Auflisten			
ListPolicyGrants [nur Berechtigung]	Erteilt die Berechtigung, Richtlinienzuschüsse aufzulisten	Auflisten			
ListProjectMemberships	Gewährt die Berechtigung zum Auflisten von Projektmitgliedern	Auflisten			
ListProjects	Gewährt die Berechtigung zum Auflisten von Projekten.	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListSubscriptionGrants	Gewährt die Berechtigung zum Auflisten von Abonnementgewährungen für einen abonnierten Prinzipal	Auflisten			
ListSubscriptionRequests	Gewährt die Berechtigung zum Auflisten von Abonnementanforderungen	Auflisten			
ListSubscriptionTargets	Gewährt die Berechtigung zum Auflisten von Abonnementzielen	Auflisten			
ListSubscriptions	Gewährt die Berechtigung zum Auflisten von Abonnements	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Abrufen aller Tags, die einer Ressource zugeordnet sind.	Lesen	domain		
ListTimeSeriesDataPoints	Erteilt die Erlaubnis, bestehende aufzulisten TimeSeriesDataPoints	Auflisten			
ListWarehouseMetadata [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der verfügbaren Manager Secrets	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PostTimeSeriesDataPoints	Erteilt die Erlaubnis, ein neues zu posten TimeSeriesDataPoints	Schreiben			
ProvisionDomain [nur Berechtigung]	Gewährt die Berechtigung zum Bereitstellen einer Domain mit standardmäßiger Projekteinrichtung	Schreiben			
PutDomainSharingPolicy [nur Berechtigung]	Erteilt die Berechtigung zum Hinzufügen einer Ressourcenrichtlinie für eine DataZone Domain	Berechtigungsverwaltung			
PutEnvironmentBlueprintConfiguration	Gewährt die Berechtigung zum Ablegen einer Umgebungsvorlagenkonfiguration	Schreiben			
RefreshToken [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren eines Tokens	Schreiben			
RejectPredictions	Gewährt die Berechtigung zum Ablehnen einer Vorhersage	Schreiben			
RejectSubscriptionRequest	Gewährt die Berechtigung zum Ablehnen einer Abonnementanforderung nach einem Datenbestand	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RemovePolicyGrant [nur Berechtigung]	Erteilt die Erlaubnis, eine Richtlinienzuweisung zu entfernen	Schreiben			
RevokeSubscription	Gewährt die Berechtigung zum Widerrufen eines Abonnements	Schreiben			
Search	Gewährt die Berechtigung zum Durchsuchen von Datazonen-Entitäten	Auflisten			
SearchGroupProfiles	Erteilt die Berechtigung zum Durchsuchen von DataZone Gruppenprofilen und IAM Identity Center-Gruppen	Auflisten			
SearchListings	Gewährt die Berechtigung zum Durchsuchen von Auflistungen	Auflisten			
SearchTypes	Gewährt die Berechtigung zum Suchen nach Typen wie Bestandstypen und Formulartypen in einer Domain	Auflisten			
SearchUserProfiles	Erteilt die Berechtigung zum Durchsuchen von DataZone Benutzerprofilen, IAM Identity Center-Benutzern und DataZone IAM-Prinzipalprofilen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SsoLogin [nur Berechtigung]	Gewährt die Berechtigung zum Anmelden mit SSO	Schreiben			
SsoLogout [nur Berechtigung]	Gewährt die Berechtigung zum Abmelden mit SSO	Schreiben			
StartDataSourceRun	Erteilt die Berechtigung zum Starten eines Ausführungsjobs DataSource	Schreiben			
StartMetadataGenerationRun	Gewährt die Berechtigung zum Starten eines Metadatengenerierungslaufs	Schreiben			
StopMetadataGenerationRun	Gewährt die Berechtigung zum Stoppen eines Metadatengenerierungslaufs	Schreiben			
TagResource	Gewährt die Berechtigung zum Hinzufügen oder Aktualisieren von Tags zu einer Ressource	Tagging	domain*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags, die einer Ressource zugeordnet sind.	Tagging	domain*		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateDataSource	Erteilt die Erlaubnis, bestehende zu aktualisieren DataSource	Schreiben			
UpdateDataSourceRunActivities [nur Berechtigung]	Erteilt die Berechtigung zum Aktualisieren von ausgeführten Aktivitäten der Datenquelle	Schreiben			
UpdateDomain	Gewährt die Berechtigung zum Aktualisieren der Informationen für eine Domain	Schreiben	domain*		
UpdateEnvironment	Gewährt die Berechtigung zum Aktualisieren von Umgebungseinstellungen	Schreiben			
UpdateEnvironmentBlueprint [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren von Umgebungsvorlageneinstellungen	Schreiben			
UpdateEnvironmentConfiguration [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren einer Umgebungskonfiguration	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateEnvironmentDeploymentStatus [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren des Status einer Umgebungsbereitstellung.	Schreiben			
UpdateEnvironmentProfile	Erteilt die Berechtigung zum Aktualisieren der EnvironmentProfile Konfiguration	Schreiben			
UpdateGlossary	Gewährt die Berechtigung zum Aktualisieren eines Geschäftsglossars	Schreiben			
UpdateGlossaryTerm	Gewährt die Berechtigung zum Aktualisieren eines Glossarbegriffs	Schreiben			
UpdateGroupProfile	Erteilt die Berechtigung zum Aktualisieren eines DataZone Gruppenprofils	Schreiben			
UpdateProject	Gewährt die Berechtigung zum Aktualisieren eines Projekts, das Ihrem Team ermöglicht, Daten zu veröffentlichen und zu abonnieren	Schreiben			
UpdateSubscriptionGrantStatus	Gewährt die Berechtigung zum Aktualisieren eines Abonnementgewährungszustands für benutzerdefinierte Gewährungen	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateSubscriptionRequest	Gewährt die Berechtigung zum Aktualisieren eines Geschäftsgrunds für eine Abonnementanforderung nach einem Datenbestand	Schreiben			
UpdateSubscriptionTarget	Gewährt die Berechtigung zum Aktualisieren eines Abonnementziels	Schreiben			
UpdateUserProfile	Erteilt die Berechtigung zum Aktualisieren eines DataZone Benutzerprofils	Schreiben			
ValidatePassRole [nur Berechtigung]	Gewährt die Berechtigung zum Validieren einer Passrichtlinie	Schreiben			

Von Amazon definierte Ressourcentypen DataZone

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
domain	`arn:${Partition}:datazone:${Region}:${Account}:domain/${DomainId}`	aws:ResourceTag/${TagKey}

Zustandsschlüssel für Amazon DataZone

Amazon DataZone definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Deadline Cloud

AWS Deadline Cloud (Dienstpräfix:`deadline`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Deadline Cloud definierte Aktionen

- Von AWS Deadline Cloud definierte Ressourcentypen
- Bedingungsschlüssel für AWS Deadline Cloud

Von AWS Deadline Cloud definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateMemberToFarm	Erteilt die Erlaubnis, ein Mitglied einer Farm zuzuordnen	Berechtigungsverwaltung	farm*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	
AssociateMemberToFleet	Erteilt die Erlaubnis, ein Mitglied einer Flotte zuzuordnen	Berechtigungsverwaltung	fleet*		identitystore:DescribeGroup identitystore:DescribeUser

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	
AssociateMemberToJob	Erteilt die Erlaubnis, ein Mitglied einem Job zuzuordnen	Berechtigungsverwaltung	job*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	
AssociateMemberToQueue	Erteilt die Berechtigung, ein Mitglied einer Warteschlange zuzuordnen	Berechtigungsverwaltung	queue*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssumeFleetRoleForRead	Erteilt die Berechtigung, eine Flottenrolle für schreibgeschützten Zugriff zu übernehmen	Schreiben	fleet*		identitystore:ListGroupMembershipsForMember
AssumeFleetRoleForWorker	Erteilt einem Arbeiter die Erlaubnis, eine Flottenrolle zu übernehmen	Schreiben	worker*		
AssumeQueueRoleForRead	Erteilt die Berechtigung, eine Warteschlangenrolle für schreibgeschützten Zugriff zu übernehmen	Schreiben	queue*		identitystore:ListGroupMembershipsForMember
AssumeQueueRoleForUser	Erteilt einem Benutzer die Berechtigung, eine Warteschlangenrolle zu übernehmen	Schreiben	queue*		identitystore:ListGroupMembershipsForMember
AssumeQueueRoleForWorker	Erteilt einem Mitarbeiter die Erlaubnis, eine Warteschlangenrolle zu übernehmen	Schreiben	queue* worker*		
BatchGetJobEntity	Erteilt einer Arbeitskraft die Erlaubnis, eine Job-Entität abzurufen	Lesen	worker*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CopyJobTemplate	Erteilt die Erlaubnis, eine Jobvorlage in einen Amazon S3 S3-Bucket zu kopieren	Schreiben	job*		identitystore:ListGroupMembershipsForMember s3:PutObject
CreateBudget	Erteilt die Erlaubnis, ein Budget zu erstellen	Schreiben	budget*		identitystore:ListGroupMembershipsForMember
CreateFarm	Erteilt die Erlaubnis zum Erstellen einer Farm	Schreiben	farm*		deadline:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateFleet	Gewährt die Berechtigung zum Erstellen einer Flotte	Schreiben	fleet*		deadline:TagResource iam:PassRole identitystore:ListGroupMembershipsForMember logs:CreateLogGroup
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateJob	Gewährt die Berechtigung zum Erstellen eines Auftrags.	Schreiben	job*		identitystore:ListGroupMembershipsForMember

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateLicenseEndpoint	Erteilt die Berechtigung zum Erstellen eines Lizenzendpunkts für lizenzierte Software oder Produkte	Schreiben	license-endpoint*		deadline:TagResource ec2:CreateTags ec2:CreateVpcEndpoint ec2:DescribeVpcEndpoints
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateMonitor	Gewährt die Berechtigung zum Erstellen eines Monitors	Schreiben	monitor*		iam:PassRole sso:CreateApplication sso:DeleteApplication sso:PutApplicationAssignmentConfiguration sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateQueue	Erteilt die Berechtigung zum Erstellen einer Warteschlange	Schreiben	queue*		deadline:TagResource iam:PassRole identitystore:ListGroupMembershipsForMember logs:CreateLogGroup s3:ListBucket
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateQueueEnvironment	Erteilt die Berechtigung zum Erstellen einer Warteschlangenumgebung	Schreiben	queue*		identitystore:ListGroupMembershipsForMember

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateQueueFleetAssociation	Erteilt die Berechtigung zum Erstellen einer Zuordnung zwischen Warteschlangen und Flotten	Schreiben	fleet*		identitystore:ListGroupMembershipsForMember
			queue*		
CreateStorageProfile	Erteilt die Berechtigung zum Erstellen eines Speicherprofils für eine Farm	Schreiben	farm*		identitystore:ListGroupMembershipsForMember
CreateWorker	Gewährt die Berechtigung zum Erstellen eines Workers	Schreiben	worker*		
DeleteBudget	Erteilt die Berechtigung zum Löschen eines Budgets	Schreiben	budget*		identitystore:ListGroupMembershipsForMember
DeleteFarm	Erteilt die Berechtigung zum Löschen einer Farm	Schreiben	farm*		identitystore:ListGroupMembershipsForMember

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteFleet	Gewährt die Berechtigung zum Löschen einer Flotte	Schreiben	fleet*		identitystore:ListGroupMembershipsForMember
DeleteLicenseEndpoint	Erteilt die Berechtigung zum Löschen eines Lizenzendpunkts	Schreiben	license-endpoint*		ec2:DeleteVpcEndpoints ec2:DescribeVpcEndpoints
DeleteMeteredProduct	Erteilt die Erlaubnis zum Löschen eines Produkts mit Nutzungsdauer	Schreiben	metered-product*		
DeleteMonitor	Gewährt die Berechtigung zum Löschen eines Monitors	Schreiben	monitor*		sso:DeleteApplication
DeleteQueue	Erteilt die Berechtigung zum Löschen einer Warteschlange	Schreiben	queue*		identitystore:ListGroupMembershipsForMember
DeleteQueueEnvironment	Erteilt die Berechtigung zum Löschen einer Warteschlangenumgebung	Schreiben	queue*		identitystore:ListGroupMembershipsForMember

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteQueueFleetAssociation	Erteilt die Berechtigung zum Löschen einer Zuordnung zwischen Warteschlangen und Flotten	Schreiben	fleet*		identitystore:ListGroupMembershipsForMember
			queue*		
DeleteStorageProfile	Erteilt die Berechtigung zum Löschen eines Speicherprofils	Schreiben	farm*		identitystore:ListGroupMembershipsForMember
DeleteWorker	Gewährt die Berechtigung zum Löschen eines Workers	Schreiben	worker*		
DisassociateMemberFromFarm	Erteilt die Berechtigung, die Zuordnung eines Mitglieds zu einer Farm aufzuheben	Berechtigungsverwaltung	farm*		identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel	
DisassociateMemberFromFleet	Erteilt die Erlaubnis, die Zuordnung eines Mitglieds zu einer Flotte aufzuheben	Berechtigungsverwaltung	fleet*		identitystore:ListGroupMembershipsForMember

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				deadline:AssociatedMembershipLevel	
DisassociateMemberFromJob	Erteilt die Erlaubnis, einem Mitglied die Zuordnung zu einem Job zu entziehen	Berechtigungsverwaltung	job*		identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel	
DisassociateMemberFromQueue	Erteilt die Berechtigung, ein Mitglied von einer Warteschlange zu trennen	Berechtigungsverwaltung	queue*		identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel	
GetApplicationVersion	Erteilt die Berechtigung, die neueste Version einer Anwendung abzurufen	Lesen	monitor*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBudget	Erteilt die Erlaubnis, ein Budget zu erhalten	Lesen	budget*		identitystore:ListGroupMembershipsForMember
GetFarm	Erteilt die Erlaubnis, eine Farm zu erwerben	Lesen	farm*		identitystore:ListGroupMembershipsForMember
GetFleet	Erteilt die Erlaubnis, eine Flotte zu erwerben	Lesen	fleet*		identitystore:ListGroupMembershipsForMember
GetJob	Erteilt die Erlaubnis, einen Job zu bekommen	Lesen	job*		identitystore:ListGroupMembershipsForMember
GetLicenseEndpoint	Erteilt die Erlaubnis, einen Lizenzendpunkt abzurufen	Lesen	license-endpoint*		
GetMonitor	Erteilt die Erlaubnis, einen Monitor zu erhalten	Lesen	monitor*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetQueue	Erteilt die Erlaubnis, eine Warteschlange abzurufen	Lesen	queue*		identitystore:ListGroupMembershipsForMember
GetQueueEnvironment	Erteilt die Erlaubnis, eine Warteschlangenumgebung abzurufen	Lesen	queue*		identitystore:ListGroupMembershipsForMember
GetQueueFleetAssociation	Erteilt die Erlaubnis, eine Zuordnung zwischen Warteschlangen und Flotten herzustellen	Lesen	fleet*		identitystore:ListGroupMembershipsForMember
			queue*		
GetSession	Erteilt die Erlaubnis, eine Sitzung für einen Job zu starten	Lesen	job*		identitystore:ListGroupMembershipsForMember
GetSessionAction	Erteilt die Berechtigung, eine Sitzungsaktion für einen Job abzurufen	Lesen	job*		identitystore:ListGroupMembershipsForMember

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetSessionsStatisticsAggregation	Erteilt die Erlaubnis, alle gesammelten Statistiken für Sitzungen abzurufen	Lesen	farm		identitystore:ListGroupMembershipsForMember
			fleet		
			queue		
GetStep	Erteilt die Erlaubnis, einen Schritt in einem Job zu erhalten	Lesen	job*		identitystore:ListGroupMembershipsForMember
GetStorageProfile	Erteilt die Erlaubnis zum Abrufen eines Speicherprofils	Lesen	farm*		identitystore:ListGroupMembershipsForMember
GetStorageProfileForQueue	Erteilt die Berechtigung zum Abrufen eines Speicherprofils für eine Warteschlange	Lesen	queue*		identitystore:ListGroupMembershipsForMember
GetTask	Erteilt die Erlaubnis, eine Auftragsaufgabe abzurufen	Lesen	job*		identitystore:ListGroupMembershipsForMember

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetWorker	Gewährt Berechtigungen zum Abrufen eines Workers	Lesen	worker*		identitystore:ListGroupMembershipsForMember
ListAvailableMeteredProducts	Erteilt die Berechtigung, alle verfügbaren Produkte mit begrenzter Nutzungsdauer innerhalb eines Lizenzendpunkts aufzulisten	Auflisten			
ListBudgets	Erteilt die Berechtigung, alle Budgets für eine Farm aufzulisten	Auflisten	budget*		identitystore:ListGroupMembershipsForMember
ListFarmMembers	Erteilt die Berechtigung, alle Mitglieder einer Farm aufzulisten	Auflisten	farm*		identitystore:ListGroupMembershipsForMember

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListFarms	Erteilt die Berechtigung, alle Farmen aufzulisten	Auflisten	farm*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:PrincipalId deadline:RequesterPrincipalId	
ListFleetMembers	Erteilt die Erlaubnis, alle Mitglieder einer Flotte aufzulisten	Auflisten	fleet*		identitystore:ListGroupMembershipsForMember

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListFleets	Gewährt die Berechtigung zum Auflisten von Flotten	Auflisten	fleet*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:PrincipalId deadline:RequesterPrincipalId	
ListJobMembers	Erteilt die Berechtigung, alle Mitglieder eines Jobs aufzulisten	Auflisten	job*		identitystore:ListGroupMembershipsForMember

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListJobs	Erteilt die Berechtigung, alle Jobs in einer Warteschlange aufzulisten	Auflisten	job*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:PrincipalId deadline:RequesterPrincipalId	
ListLicenseEndpoints	Erteilt die Berechtigung, alle Lizenzendpunkte aufzulisten	Auflisten	license-endpoint*		
ListMeteredProducts	Erteilt die Erlaubnis, alle Produkte, für die eine Nutzungsdauer gilt, auf einem Lizenzendpunkt aufzulisten	Auflisten	metered-product*		
ListMonitors	Erteilt die Erlaubnis, alle Monitore aufzulisten	Auflisten	monitor*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListQueueEnvironments	Erteilt die Berechtigung, alle Warteschlangenumgebungen aufzulisten, denen eine Warteschlange zugeordnet ist	Auflisten	queue*		identitystore:ListGroupMembershipsForMember
ListQueueFleetAssociations	Erteilt die Berechtigung, alle Verbindungen zwischen Warteschlangen und Flotten aufzulisten	Auflisten	farm		identitystore:ListGroupMembershipsForMember
			fleet		
			queue		
ListQueueMembers	Erteilt die Berechtigung, alle Mitglieder einer Warteschlange aufzulisten	Auflisten	queue*		identitystore:ListGroupMembershipsForMember

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListQueues	Erteilt die Berechtigung, alle Warteschlangen in einer Farm aufzulisten	Auflisten	queue*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:PrincipalId deadline:RequesterPrincipalId	
ListSessionActions	Erteilt die Berechtigung, alle Sitzungsaktionen für einen Job aufzulisten	Auflisten	job*		identitystore:ListGroupMembershipsForMember

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListSessions	Erteilt die Berechtigung, alle Sitzungen für einen Job aufzulisten	Auflisten	job*		identitystore:ListGroupMembershipsForMember
ListSessionsForWorker	Erteilt die Berechtigung, alle Sitzungen einer Arbeitskraft aufzulisten	Auflisten	worker*		identitystore:ListGroupMembershipsForMember
ListStepConsumers	Erteilt die Berechtigung, die Schrittverbraucher für einen Arbeitsschritt aufzulisten	Auflisten	job*		identitystore:ListGroupMembershipsForMember
ListStepDependencies	Erteilt die Berechtigung, Abhängigkeiten für einen Job-Schritt aufzulisten	Auflisten	job*		identitystore:ListGroupMembershipsForMember
ListSteps	Erteilt die Berechtigung, alle Schritte für einen Job aufzulisten	Auflisten	job*		identitystore:ListGroupMembershipsForMember

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListStorageProfiles	Erteilt die Berechtigung, alle Speicherprofile in einer Farm aufzulisten	Auflisten	farm*		identitystore:ListGroupMembershipsForMember
ListStorageProfilesForQueue	Erteilt die Berechtigung, alle Speicherprofile in einer Warteschlange aufzulisten	Auflisten	queue*		identitystore:ListGroupMembershipsForMember
ListTagsForResource	Erteilt die Berechtigung, alle Tags auf bestimmten Deadline Cloud-Ressourcen aufzulisten	Auflisten	farm		
			fleet		
			license-endpoint		
			queue		
ListTasks	Erteilt die Erlaubnis, alle Aufgaben für einen Job aufzulisten	Auflisten	job*		identitystore:ListGroupMembershipsForMember
ListWorkers	Erteilt die Erlaubnis, alle Arbeiter einer Flotte aufzulisten	Auflisten	worker*		identitystore:ListGroupMembershipsForMember

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutMeteredProduct	Erteilt die Erlaubnis, einem Lizenzendpunkt ein Produkt mit begrenzter Nutzungsdauer hinzuzufügen	Schreiben	metered-product*		
SearchJobs	Erteilt die Berechtigung, in mehreren Warteschlangen nach Aufträgen zu suchen	Auflisten	queue*		identitystore:ListGroupMembershipsForMember
SearchSteps	Erteilt die Berechtigung, die Schritte innerhalb eines einzelnen Jobs oder die Schritte in mehreren Warteschlangen zu durchsuchen	Auflisten	job		identitystore:ListGroupMembershipsForMember
			queue		
SearchTasks	Erteilt die Berechtigung, die Aufgaben innerhalb eines einzelnen Auftrags oder die Aufgaben nach mehreren Warteschlangen zu durchsuchen	Auflisten	job		identitystore:ListGroupMembershipsForMember
			queue		
SearchWorkers	Erteilt die Berechtigung, nach Arbeitskräften in mehreren Flotten zu suchen	Auflisten	fleet*		identitystore:ListGroupMembershipsForMember

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartSessionsStatisticsAggregation	Erteilt die Erlaubnis, alle gesammelten Statistiken für Sitzungen abzurufen	Lesen	fleet		identitystore:ListGroupMembershipsForMember
			queue		
TagResource	Erteilt die Berechtigung, ein oder mehrere Tags für die angegebene Deadline Cloud-Ressource hinzuzufügen oder zu überschreiben	Tagging	farm		
			fleet		
			license-endpoint		
			queue		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Erteilt die Berechtigung, die Zuordnung eines oder mehrerer Tags zur angegebenen Deadline Cloud-Ressource aufzuheben	Tagging	farm		
			fleet		
			license-endpoint		
			queue		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateBudget	Erteilt die Erlaubnis, ein Budget zu aktualisieren	Schreiben	budget*		identitystore:ListGroupMembershipsForMember
UpdateFarm	Erteilt die Erlaubnis, eine Farm zu aktualisieren	Schreiben	farm*		identitystore:ListGroupMembershipsForMember
UpdateFleet	Erteilt die Erlaubnis, eine Flotte zu aktualisieren	Schreiben	fleet*		iam:PassRole identitystore:ListGroupMembershipsForMember
UpdateJob	Gewährt die Berechtigung zum Aktualisieren eines Auftrags.	Schreiben	job*		identitystore:ListGroupMembershipsForMember

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateMonitor	Gewährt die Berechtigung zum Aktualisieren eines Monitors	Schreiben	monitor*		iam:PassRole sso:PutApplicationGrant sso:UpdateApplication
UpdateQueue	Erteilt die Erlaubnis, eine Warteschlange zu aktualisieren	Schreiben	queue*		iam:PassRole identitystore:ListGroupMembershipsForMember
UpdateQueueEnvironment	Erteilt die Berechtigung zum Aktualisieren einer Warteschlangenumgebung	Schreiben	queue*		identitystore:ListGroupMembershipsForMember
UpdateQueueFleetAssociation	Erteilt die Erlaubnis, eine Verbindung zwischen Warteschlangen und Flotten zu aktualisieren	Schreiben	fleet*		identitystore:ListGroupMembershipsForMember
			queue*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateSession	Erteilt die Berechtigung, eine Sitzung für einen Job zu aktualisieren	Schreiben	job*		identitystore:ListGroupMembershipsForMember
UpdateStep	Erteilt die Berechtigung, einen Schritt für einen Job zu aktualisieren	Schreiben	job*		identitystore:ListGroupMembershipsForMember
UpdateStorageProfile	Erteilt die Berechtigung zum Aktualisieren eines Speicherprofils für eine Farm	Schreiben	farm*		identitystore:ListGroupMembershipsForMember
UpdateTask	Gewährt die Berechtigung zum Aktualisieren einer Aufgabe	Schreiben	job*		identitystore:ListGroupMembershipsForMember
UpdateWorker	Gewährt die Berechtigung zum Aktualisieren eines Workers	Schreiben	worker*		logs:CreateLogStream
UpdateWorkerSchedule	Erteilt die Berechtigung, den Zeitplan für eine Arbeitskraft zu aktualisieren	Schreiben	worker*		logs:CreateLogStream

Von AWS Deadline Cloud definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
budget	`arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/budget/${BudgetId}`	deadline:FarmMembershipLevels
farm	`arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}`	aws:ResourceTag/${TagKey} deadline:FarmMembershipLevels
fleet	`arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/fleet/${FleetId}`	aws:ResourceTag/${TagKey} deadline:FarmMembershipLevels deadline:FleetMembershipLevels
job	`arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/queue/${QueueId}/job/${JobId}`	deadline:FarmMembershipLevels deadline:JobMembershipLevels deadline:QueueMembershipLevels

Ressourcentypen	ARN	Bedingungsschlüssel
license-endpoint	`arn:${Partition}:deadline:${Region}:${Account}:license-endpoint/${LicenseEndpointId}`	aws:ResourceTag/${TagKey}
metered-product	`arn:${Partition}:deadline:${Region}:${Account}:license-endpoint/${LicenseEndpointId}/metered-product/${ProductId}`	
monitor	`arn:${Partition}:deadline:${Region}:${Account}:monitor/${MonitorId}`	
queue	`arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/queue/${QueueId}`	aws:ResourceTag/${TagKey} deadline:FarmMembershipLevels deadline:QueueMembershipLevels
worker	`arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/fleet/${FleetId}/worker/${WorkerId}`	deadline:FarmMembershipLevels deadline:FleetMembershipLevels

Bedingungsschlüssel für AWS Deadline Cloud

AWS Deadline Cloud definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString
deadline:AssociatedMembershipLevel	Filtert den Zugriff nach der zugehörigen Mitgliedschaftsstufe des in der Anfrage angegebenen Prinzipals	String
deadline:FarmMembershipLevels	Filtert den Zugriff nach Mitgliedschaftsstufen in der Farm	ArrayOfString
deadline:FleetMembershipLevels	Filtert den Zugriff nach Mitgliedschaftsstufen auf der Flotte	ArrayOfString
deadline:JobMembershipLevels	Filtert den Zugriff nach Mitgliedschaftsstufen im Job	ArrayOfString
deadline:MembershipLevel	Filtert den Zugriff nach der Mitgliedschaftsstufe, die in der Anfrage angegeben wurde	String
deadline:PrincipalId	Filtert den Zugriff nach der in der Anfrage angegebenen Prinzipien-ID	String

Bedingungsschlüssel	Beschreibung	Typ
deadline:QueueMembershipLevels	Filtert den Zugriff nach Mitgliedschaftsstufen in der Warteschlange	ArrayOfString
deadline:RequesterPrincipalId	Filtert den Zugriff durch den Benutzer, der die Deadline Cloud-API aufruft	String

Aktionen, Ressourcen und Bedingungsschlüssel für AWS DeepComposer

AWS DeepComposer (Servicepräfix: `deepcomposer`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS DeepComposer definierte Aktionen
- Von AWS DeepComposer definierte Ressourcentypen
- Bedingungsschlüssel für AWS DeepComposer

Von AWS DeepComposer definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Associate Coupon [nur Berechtigung]	Gewährt die Berechtigung zum Zuordnen eines DeepComposer-Coupon (oder DSN) zu dem Konto, das dem Sender der Anfrage zugeordnet ist	Write			
CreateAudio [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer Audiodatei, indem die Midi-Komposition in eine WAV- oder MP3-Datei konvertiert wird	Write	audio*		
CreateComposition [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer Mehrspur-Midi-Komposition	Write	composition*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModel [nur Berechtigung]	Gewährt die Berechtigung, mit der Erstellung/Übung eines generativen Modells zu beginnen, das in der Lage ist, Inferenz gegen die vom Benutzer bereitgestellte Klaviermelodie durchzuführen, um eine mehrspurige Midi-Komposition zu erstellen	Write	model*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteComposition [nur Berechtigung]	Gewährt die Berechtigung zum Löschen der Komposition	Write	composition*		
DeleteModel	Gewährt die Berechtigung zum Löschen des Modells	Write	model*		
GetComposition [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Informationen zu der Komposition	Read	composition*		
				aws:ResourceTag/${TagKey}	
GetModel [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Informationen zu dem Modell	Read	model*		
				aws:ResourceTag/${TagKey}	
GetSampleModel [nur Berechtigung]	Gewährt die Berechtigung, Informationen über das Beispiel/vortrainierte DeepComposer-Modell zu erhalten	Read	model*		
ListCompositions [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aller Kompositionen, die dem Sender der Anforderung gehören	List	composition*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListModels [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aller Modelle, die dem Sender der Anfrage gehören	List	model*		
ListSampleModels [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aller Beispiel-/vortrainierten Modelle, die vom DeepComposer-Service bereitgestellt werden.	List	model*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	List	composition		
			model		
				aws:ResourceTag/${TagKey}	
ListTrainingTopics [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aller Übungsoptionen oder Themen zum Erstellen/Üben eines Modells	List	model*		
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren	composition		
			model		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Markieren	composition		
			model		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateComposition [nur Berechtigung]	Gewährt die Berechtigung zum Ändern der veränderbaren Eigenschaften, die mit einer Komposition verknüpft sind	Write	composition*		
UpdateModel [nur Berechtigung]	Gewährt die Berechtigung zum Ändern der veränderbaren Eigenschaften, die mit einem Modell verknüpft sind	Write	model*		

Von AWS DeepComposer definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
model	`arn:${Partition}:deepcomposer:${Region}:${Account}:model/${ModelId}`	aws:ResourceTag/${TagKey}
composition	`arn:${Partition}:deepcomposer:${Region}:${Account}:composition/${CompositionId}`	aws:ResourceTag/${TagKey}
audio	`arn:${Partition}:deepcomposer:${Region}:${Account}:audio/${AudioId}`	

Bedingungsschlüssel für AWS DeepComposer

AWS DeepComposer definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff danach, ob Tag-Schlüssel-Wert-Paare in der Anforderung vorhanden sind	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tag-Schlüssel-Wert-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert Zugriff basierend auf dem Vorhandensein von Tag-Schlüsseln in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS DeepLens

AWS DeepLens (Servicepräfix: `deeplens`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Themen

- Von AWS DeepLens definierte Aktionen
- Von AWS DeepLens definierte Ressourcentypen
- Bedingungsschlüssel für AWS DeepLens

Von AWS DeepLens definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie

den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateServiceRoleToAccount	Verknüpft das Konto des Benutzers mit IAM-Rollen, mit denen verschiedene Berechtigungen gesteuert werden, die AWS DeepLens für die ordnungsgemäße Funktionalität benötigt.	Berechtigungsverwaltung			
BatchGetDevice	Ruft eine Liste der AWS DeepLens-Geräte ab.	Read	device*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetModel	Ruft eine Liste der AWS DeepLens-Modelle ab.	Read	model*		
BatchGetProject	Ruft eine Liste der AWS DeepLens-Projekte ab.	Read	project*		
CreateDeviceCertificates	Erstellt ein Zertifikatpaket, das zum erfolgreichen Authentifizieren und Registrieren eines AWS DeepLens-Geräts verwendet wird.	Write			
CreateModel	Erstellt ein neues AWS DeepLens-Modell.	Write			
CreateProject	Erstellt ein neues AWS DeepLens-Projekt.	Write			
DeleteModel	Löscht ein AWS DeepLens-Modell.	Write	model*		
DeleteProject	Löscht ein AWS DeepLens-Projekt.	Write	project*		
DeployProject	Stellt ein AWS DeepLens-Projekt für ein registriertes AWS DeepLens-Gerät bereit.	Write	device* project*		
DeregisterDevice	Beginnt einen Workflow zur Geräteabmeldung für ein registriertes AWS DeepLens-Gerät.	Write	device*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAssociatedResources	Ruft die Ressourcen auf Kontoebene ab, die mit dem Konto des Benutzers verknüpft sind.	Read			
GetDeploymentStatus	Ruft den Bereitstellungsstatus eines bestimmten AWS DeepLens-Geräts zusammen mit allen zugehörigen Metadaten ab.	Read			
GetDevice	Ruft Informationen zu einem AWS DeepLens-Gerät ab.	Read	device*		
GetModel	Ruft ein AWS DeepLens-Modell ab.	Read	model*		
GetProject	Ruft ein AWS DeepLens-Projekt ab.	Read	project*		
ImportProjectFromTemplate	Erstellt ein neues AWS DeepLens-Projekt anhand einer Musterprojektvorlage.	Write			
ListDeployments	Ruft eine Liste der AWS DeepLens-Bereitstellungs-IDs ab.	List			
ListDevices	Ruft eine Liste mit AWS DeepLens-Gerät-IDs ab.	List			
ListModels	Ruft eine Liste mit AWS DeepLens-Modell-IDs ab.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListProjects	Ruft eine Liste mit AWS DeepLens-Projekt-IDs ab.	List			
RegisterDevice	Beginnt einen Workflow zur Geräteregistrierung für ein AWS DeepLens-Gerät.	Write			
RemoveProject	Entfernt ein bereitgestelltes AWS DeepLens-Projekt von einem AWS DeepLens-Gerät.	Write	device*		
UpdateProject	Aktualisiert ein bestehende AWS DeepLens-Projekt.	Write	project*		

Von AWS DeepLens definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
device	`arn:${Partition}:deeplens:${Region}:${Account}:device/${DeviceName}`	
project	`arn:${Partition}:deeplens:${Region}:${Account}:project/${ProjectName}`	

Ressource ntypen	ARN	Bedingungsschlüssel
model	`arn:${Partition}:deeplens:${Region}:${Account}:model/${ModelName}`	

Bedingungsschlüssel für AWS DeepLens

DeepLens besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS DeepRacer

AWS DeepRacer (Service-Präfix: `deepracer`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS DeepRacer definierte Aktionen
- Von AWS DeepRacer definierte Ressourcentypen
- Bedingungsschlüssel für AWS DeepRacer

Von AWS DeepRacer definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddLeaderboardAcce	Gewährt die Berechtigung zum Hinzufügen des Zugriffs	Write	leaderboard*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ssPermission [nur Berechtigung]	zu einem privaten Bestenboards.			deepracer:UserToken deepracer:MultiUser	
AdminGetAccountConfig [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen der aktuellen Administratorkonfiguration für dieses Konto	Lesen			
AdminListAssociatedResources [nur Berechtigung]	Gewährt die Berechtigung, alle Deepracer-Benutzer mit ihren zugeordneten Ressourcen aufzulisten, die unter diesem Konto erstellt wurden	Lesen			
AdminListAssociatedUsers [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Benutzerdaten für alle Benutzer, die diesem Konto zugeordnet sind	Lesen			
AdminManageUser [nur Berechtigung]	Gewährt die Berechtigung zum Verwalten eines Benutzers, der diesem Konto zugeordnet ist	Schreiben			
AdminSetAccountConfig [nur Berechtigung]	Gewährt die Berechtigung zum Festlegen von Konfigurationsoptionen für dieses Konto	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CloneReinforcementLearningModel [nur Berechtigung]	Gewährt die Berechtigung zum Klonen vorhandener DeepRacer-Modelle.	Write	reinforcement_learning_model*		
			track*		
				aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCar [nur Berechtigung]	Gewährt die Berechtigung, ein DeepRacer Auto in Ihrer Garage zu erstellen	Write		aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	
CreateLeaderboard [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer Bestenliste	Write		aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateLeaderboardAccessToken [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines Zugriffstoken für eine private Rangliste	Write	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
CreateLeaderboardSubmission [nur Berechtigung]	Gewährt die Berechtigung zum Einreichen von DeepRacer-Modellen, die für Ranglisten ausgewertet werden.	Write	leaderboard*		
			reinforcement_learning_model*		
				aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateReinforcementLearningModel [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen von Reinforcement-Learning-Modellen für DeepRacer.	Write	track*		
				aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	
DeleteLeaderboard [nur Berechtigung]	Gewährt die Berechtigung zum Löschen einer Bestenliste	Write	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
DeleteModel [nur Berechtigung]	Gewährt die Berechtigung zum Löschen von DeepRacer-Modellen.	Write	reinforcement_learning_model*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				deepracer:UserToken deepracer:MultiUser	
EditLeaderboard [nur Berechtigung]	Gewährt die Berechtigung zum Bearbeiten einer Bestenliste	Write	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
GetAccountConfig [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen der aktuellen Mehrbenutzerkonfiguration für dieses Konto	Lesen		deepracer:UserToken deepracer:MultiUser	
GetAlias [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen des Alias des Benutzers für das Einreichten von DeepRacer-Modellen für eine Rangliste.	Read		deepracer:UserToken deepracer:MultiUser	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAssetUrl [nur Berechtigung]	Gewährt die Berechtigung zum Download von Artifacts für ein vorhandenes DeepRacer-Modell	Read	reinforcement_learning_model*		
				deepracer:UserToken deepracer:MultiUser	
GetCar [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen eines bestimmten DeepRacer Autos aus Ihrer Garage	Read	car*		
				deepracer:UserToken deepracer:MultiUser	
GetCars [nur Berechtigung]	Gewährt die Berechtigung, alle DeepRacer Autos in Ihrer Garage zu sehen	Read		deepracer:UserToken deepracer:MultiUser	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetEvaluation [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Informationen zu den Auswertungsaufträgen vorhandener DeepRacer-Modelle.	Read	evaluation_job*		
				deepracer:UserToken deepracer:MultiUser	
GetLatestUserSubmission [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Informationen zur Leistung des zuletzt eingereichten DeepRacer-Modells eines Benutzers in einer Rangliste.	Read	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
GetLeaderboard [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Informationen zu Ranglisten.	Read	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetModel [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Informationen zu vorhandenen DeepRacer-Modellen.	Read	reinforcement_learning_model*		
				deepracer:UserToken deepracer:MultiUser	
GetPrivateLeaderboard [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Informationen zu privaten Ranglisten.	Read	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
GetRankedUserSubmission [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Informationen zur Leistung des DeepRacer-Modells eines Benutzers, das in einer Rangliste platziert ist.	Read	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetTrack [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Informationen zu DeepRacer-Strecken.	Read	track*		
GetTrainingJob [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Informationen zum Trainingsauftrag vorhandener DeepRacer-Modelle.	Read	training_job*		
				deepracer:UserToken deepracer:MultiUser	
ImportModel [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen von Reinforcement-Learning-Modellen für DeepRacer.	Write		deepracer:UserToken deepracer:MultiUser	
ListEvaluations [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der Auswertungsaufträge von DeepRacer-Modellen.	Read	reinforcement_learning_model*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				deepracer:UserToken deepracer:MultiUser	
ListLeaderboardEvaluations [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aller Bewertungsaufträge des Benutzers für die Rangliste	Lesen	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
ListLeaderboardSubmissions [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aller Beiträge von DeepRacer-Modellen eines Benutzers in einer Rangliste.	Read	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListLeaderboards [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aller verfügbaren Ranglisten.	Read		deepracer:UserToken deepracer:MultiUser	
ListModels [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aller vorhandenen DeepRacer-Modelle.	Read		deepracer:UserToken deepracer:MultiUser	
ListPrivateLeaderboardParticipants [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Teilnehmerinformationen zu Ranglisten.	Read	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
ListPrivateLeaderboards [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aller verfügbaren privaten Ranglisten.	Read		deepracer:UserToken deepracer:MultiUser	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListSubscribedPrivateLeaderboards [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aller abonnierten privaten Ranglisten	Lesen		deepracer:UserToken deepracer:MultiUser	
ListTagsForResource	Gewährt die Berechtigung zum Auflisten des Tags für eine Ressource.	Lesen	car		
			evaluation_job		
			leaderboard		
			leaderboard_evaluation_job		
			reinforcement_learning_model		
			training_job		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} deepracer:UserToken deepracer:MultiUser	
ListTracks [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aller DeepRacer-Strecken.	Read			
ListTrainingJobs [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der Trainingsaufträge von DeepRacer-Modellen.	Read	reinforcement_learning_model*		
				deepracer:UserToken deepracer:MultiUser	
MigrateModels [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen von Reinforcement-Learning-Modellen für DeepRacer.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PerformLeaderboardOperation [nur Berechtigung]	Gewährt die Berechtigung zum Ausführen der im Attribut Operation erwähnten Leaderboard	Schreiben	leaderboard		
				deepracer:UserToken deepracer:MultiUser	
RemoveLeaderboardAccessPermission [nur Berechtigung]	Gewährt die Berechtigung, den Zugriff für eine private Bestenliste zu entfernen	Write	leaderboard*		
				deepracer:UserToken deepracer:MultiUser	
SetAlias [nur Berechtigung]	Gewährt die Berechtigung zum Festlegen des Alias des Benutzers für das Einreichen von DeepRacer-Modellen in Ranglisten.	Write		deepracer:UserToken deepracer:MultiUser	
StartEvaluation [nur Berechtigung]	Gewährt die Berechtigung zum Auswerten von DeepRacer-Modellen in einer simulierten Umgebung.	Write	reinforcement_learning_model*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			track*		
				aws:RequestTag/${TagKey} aws:TagKeys deepracer:UserToken deepracer:MultiUser	
StopEvaluation [nur Berechtigung]	Gewährt die Berechtigung zum Beenden von DeepRacer-Modellauswertungen.	Write	evaluation_job*		
				deepracer:UserToken deepracer:MultiUser	
StopTrainingReinforcementLearningModel [nur Berechtigung]	Gewährt die Berechtigung zum Beenden des Trainings von DeepRacer-Modellen.	Schreiben	reinforcement_learning_model*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				deepracer:UserToken deepracer:MultiUser	
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren	car		
			evaluation_job		
			leaderboard		
			leaderboard_evaluation_job		
			reinforcement_learning_model		
			training_job		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} deepracer:UserToken deepracer:MultiUser	
TestRewardFunction [nur Berechtigung]	Gewährt die Berechtigung zum Testen von Belohnungsfunktionen für Richtigkeit.	Schreiben			
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Markieren	car		
			evaluation_job		
			leaderboard		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			leaderboard_evaluation_job		
			reinforcement_learning_model		
			training_job		
				aws:TagKeys deepracer:UserToken deepracer:MultiUser	
UpdateCar [nur Berechtigung]	Gewährt die Berechtigung, ein DeepRacer Auto in Ihrer Garage zu aktualisieren	Write	car*		
				deepracer:UserToken deepracer:MultiUser	

Von AWS DeepRacer definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
car	`arn:${Partition}:deepracer:${Region}:${Account}:car/${ResourceId}`	aws:ResourceTag/${TagKey}
evaluation_job	`arn:${Partition}:deepracer:${Region}:${Account}:evaluation_job/${ResourceId}`	aws:ResourceTag/${TagKey}
leaderboard	`arn:${Partition}:deepracer:${Region}::leaderboard/${ResourceId}`	aws:ResourceTag/${TagKey}
leaderboard_evaluation_job	`arn:${Partition}:deepracer:${Region}:${Account}:leaderboard_evaluation_job/${ResourceId}`	aws:ResourceTag/${TagKey}
reinforcement_learning_model	`arn:${Partition}:deepracer:${Region}:${Account}:model/reinforcement_learning/${ResourceId}`	aws:ResourceTag/${TagKey}
track	`arn:${Partition}:deepracer:${Region}::track/${ResourceId}`	
training_job	`arn:${Partition}:deepracer:${Region}:${Account}:training_job/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS DeepRacer

AWS DeepRacer definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen durch Tag-Schlüssel-Werte-Paare, die de Ressource zugeordnet sind	Zeichenfolge
aws:TagKeys	Filtert Aktionen nach den Tag-Schlüsseln in der Anforderung	ArrayOfString
deepracer:MultiUser	Filtert den Zugriff nach Mehrbenutzerflag	Bool
deepracer:UserToken	Filtert den Zugriff nach Benutzer-Token in der Anforderung	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Detective

Amazon Detective (Servicepräfix: `detective`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.

- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Detective definierte Aktionen
- Von Amazon Detective definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Detective

Von Amazon Detective definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptInvitation	Gewährt die Berechtigung, eine Einladung zur Mitgliedschaft in einem Verhaltensdiagramm anzunehmen	Schreiben			
BatchGetGraphMemberDatasources	Gewährt die Berechtigung zum Abrufen des Datenquellenpaketverlaufs für die angegebenen Mitgliedskonten in einem von diesem Konto verwalteten Verhaltensdiagramm	Lesen	Graph*		
BatchGetMembershipDatasources	Gewährt die Erlaubnis zum Abrufen der Datenquellenpaket-Historie des Anruferkontos für die angegebenen Graphen	Lesen			
CreateGraph	Gewährt die Berechtigung zum Erstellen eines Verhaltensdiagramms und beginnt mit	Write		aws:TagKeys	detective:TagResource

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	der Sammlung von Sicherheitsinformationen			aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
CreateMembers	Gewährt die Berechtigung, die Mitgliedschaft eines oder mehrerer Konten in einem von diesem Konto verwalteten Verhaltensdiagramm anzufordern	Write	Graph*		
DeleteGraph	Gewährt die Berechtigung zum Löschen eines Verhaltensdiagramms und das Beenden der Aggregation von Sicherheitsinformationen	Write	Graph*		
DeleteMembers	Gewährt die Berechtigung, Mitgliedskonten aus einem von diesem Konto verwalteten Verhaltensdiagramm zu entfernen	Schreiben	Graph*		
DescribeOrganizationConfiguration	Erteilt die Berechtigung zum Anzeigen der aktuellen Konfiguration im Zusammenhang mit der Amazon-Detective-Integration mit AWS-Organisationen	Lesen	Graph*		organizations:DescribeOrganization

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisableOrganizationAdminAccount	Gewährt die Berechtigung zum Entfernen des von Amazon Detective delegierten Administratorkontos für eine Organisation	Schreiben			organizations:DescribeOrganization
DisassociateMembership	Gewährt die Berechtigung, die Mapping dieses Kontos zu einem Verhaltensdiagramm zu entfernen	Schreiben			
EnableOrganizationAdminAccount	Gewährt die Berechtigung zum Festlegen des von Amazon Detective delegierten Administratorkontos für eine Organisation	Schreiben			iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:EnableAWSServiceAccess organizations:RegisterDelegatedAdministrator

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetFreeTrialEligibility [nur Berechtigung]	Gewährt die Berechtigung, die Berechtigung eines Verhaltensdiagramms für eine kostenlose Testphase abzurufen	Read	Graph*		
GetGraphIngestState [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen des Dateneingabestatus eines Verhaltensdiagramms.	Lesen	Graph*		
GetInvestigation	Gewährt die Berechtigung zum Abrufen des Zustands und der Metadaten einer Untersuchung	Lesen	Graph*		
GetMembers	Gewährt die Berechtigung zum Abrufen von Details zu bestimmten Mitgliedern eines Verhaltensdiagramms.	Read	Graph*		
GetPricingInformation [nur Berechtigung]	Gewährt die Berechtigung, Informationen über die Preisgestaltung von Amazon Detective abzurufen	Read			
GetUsageInformation [nur Berechtigung]	Gewährt die Berechtigung, Nutzungsinformationen eines Verhaltensdiagramms aufzulisten	Lesen	Graph*		
InvokeAssistant [nur Berechtigung]	Gewährt die Berechtigung zum Aufrufen von Detective's Assistant	Lesen	Graph*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDatasourcePackages	Ermöglicht die Auflistung der Erfassungs-Zustände des Datenquellenpakets eines Graphen und der Zeitstempel für die jüngsten Zustandsänderungen in einem von diesem Konto verwalteten Verhaltensgraphen	Auflisten	Graph*		
ListGraphs	Gewährt die Berechtigung, die von diesem Konto verwalteten Verhaltensdiagramme aufzulisten	Auflisten			
ListHighDegreeEntities [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Entitäten mit hohem Volume, deren Beziehungen von Detective nicht gespeichert werden können	Auflisten	Graph*		
ListIndicators	Gewährt die Berechtigung zum Auflisten der Indikatoren einer Untersuchung	Auflisten	Graph*		
ListInvestigations	Gewährt die Berechtigung zum Auflisten der Untersuchungen eines Verhaltensdiagramms	Auflisten	Graph*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListInvitations	Gewährt die Berechtigung, Details zu den Verhaltensdiagrammen abzurufen, zu denen dieses Konto eingeladen wurde	List			
ListMembers	Gewährt die Berechtigung, Details zu allen Mitgliedern eines Verhaltensdiagramms abzurufen	Auflisten	Graph*		
ListOrganizationAdminAccount	Gewährt die Berechtigung zum Anzeigen des von Amazon Detective delegierten Administratorkontos für eine Organisation	Auflisten			organizations:DescribeOrganization
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tag-Werte, die einem Verhaltensgraphen zugewiesen sind	Auflisten	Graph*		
				aws:ResourceTag/${TagKey}	
RejectInvitation	Gewährt die Berechtigung, eine Einladung zur Mitgliedschaft in einem Verhaltensdiagramm abzulehnen	Write			
SearchGraph [nur Berechtigung]	Gewährt die Berechtigung, die in einem Verhaltensdiagramm gespeicherten Daten zu durchsuchen	Lesen	Graph*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartInvestigation	Gewährt die Berechtigung zum Aufrufen von Untersuchungen	Schreiben	Graph*		
StartMonitoringMember	Gewährt die Berechtigung zum Starten der Datenerfassung für ein Mitgliedskonto mit dem Status ACCEPTED_BUT_DISABLED	Schreiben	Graph*		
TagResource	Gewährt die Berechtigung zum Zuweisen von Tag-Werten zu einem Verhaltensgraphen	Markieren	Graph*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tag-Werten aus einem Verhaltensgraphen	Tagging	Graph*		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateDatasourcePackages	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren von Datenquellenpaketen in einem von diesem Konto verwalteten Verhaltensdiagramm	Schreiben	Graph*		
UpdateInvestigationState	Gewährt die Berechtigung zum Aktualisieren des Zustands und der Metadaten einer Untersuchung	Schreiben	Graph*		
UpdateOrganizationConfiguration	Gewährt die Berechtigung zum Aktualisieren der aktuellen Konfiguration im Zusammenhang mit der Amazon-Detective-Integration mit AWS-Organisationen	Schreiben	Graph*		organizations:DescribeOrganization

Von Amazon Detective definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Graph	`arn:${Partition}:detective:${Region}:${Account}:graph:${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Detective

Amazon Detective definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch Angabe der Tags, die in der Anfrage übergeben werden	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff durch Angabe der Tags, die der Ressource zugeordnet sind	String
aws:TagKeys	Filtert den Zugriff durch Angabe der Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Device Farm

AWS Device Farm (Servicepräfix: `devicefarm`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.

- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Device Farm definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDevicePool	Gewährt die Berechtigung zum Erstellen eines Gerätepools innerhalb eines Projekts	Write	project*		
CreateInstanceProfile	Gewährt die Berechtigung zum Erstellen eines Instance-Profils	Write			
CreateNetworkProfile	Gewährt die Berechtigung zum Erstellen eines Netzwerkprofils innerhalb eines Projekts	Write	project*		
CreateProject	Gewährt die Berechtigung zum Erstellen eines Projekts für mobile Tests	Schreiben			ec2:CreateNetworkInterface ec2:DescribeSecurityGroups

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole
CreateRemoteAccessSession	Gewährt die Berechtigung zum Starten einer Remotezugriffssitzung für eine Geräte-Instance	Write	device*		
			project*		
			deviceinstance		
			upload		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTestGridProject	Gewährt die Berechtigung zum Erstellen eines Projekts für Desktop-Tests	Write			ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole
CreateTestGridUrl	Gewährt die Berechtigung, eine neue vorsignierte URL zu generieren, die für den Zugriff auf unseren Testraster-Service verwendet wird	Write	testgrid-project*		
CreateUpload	Gewährt die Berechtigung zum Upload einer neuen Datei oder App innerhalb eines Projekts	Write	project*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateVPCEConfiguration	Gewährt die Berechtigung zum Erstellen einer Amazon Virtual Private Cloud (VPC)-Endpunktkonfiguration	Write			
DeleteDevicePool	Gewährt die Berechtigung zum Löschen eines benutzergenerierten Gerätepools	Write	devicepool*		
DeleteInstanceProfile	Gewährt die Berechtigung zum Löschen eines benutzergenerierten Instance-Profils	Write	instanceprofile*		
DeleteNetworkProfile	Gewährt die Berechtigung zum Löschen eines benutzergenerierten Netzwerkprofils	Write	networkprofile*		
DeleteProject	Gewährt die Berechtigung zum Löschen eines mobilen Testprojekts	Write	project*		
DeleteRemoteAccessSession	Gewährt die Berechtigung zum Löschen einer abgeschlossenen Remotezugriffssitzung und ihrer Ergebnisse	Write	session*		
DeleteRun	Gewährt die Berechtigung zum Löschen einer Ausführung	Write	run*		
DeleteTestGridProject	Gewährt die Berechtigung zum Löschen eines Desktop-Testprojekts	Write	testgrid-project*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteUpload	Gewährt die Berechtigung zum Löschen einer vom Benutzer hochgeladenen Datei	Write	upload*		
DeleteVPCEConfiguration	Gewährt die Berechtigung zum Löschen einer Amazon Virtual Private Cloud (VPC)-Endpunktkonfiguration	Write	vpceconfiguration*		
GetAccountSettings	Gewährt die Berechtigung zum Abrufen der Anzahl der nicht überwachten iOS- und/oder der nicht überwachten Android-Geräte, die vom Konto gekauft wurden	Read			
GetDevice	Gewährt die Berechtigung zum Abrufen der Informationen eines eindeutigen Gerätetyps	Read	device*		
GetDeviceInstance	Gewährt die Berechtigung zum Ausmuten der Informationen einer Geräte-Instance	Read	deviceinstance*		
GetDevicePool	Gewährt die Berechtigung zum Abrufen der Informationen eines Gerätepools	Read	devicepool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDevicePoolCompatibility	Gewährt die Berechtigung zum Abrufen von Informationen zur Kompatibilität eines Tests und/oder einer App mit einem Gerätepool	Read	devicepool*		
			upload		
GetInstanceProfile	Gewährt die Berechtigung zum Abrufen der Informationen eines Instance-Profils	Read	instanceprofile*		
GetJob	Gewährt die Berechtigung zum Abrufen der Informationen einer Aufgabe	Read	job*		
GetNetworkProfile	Gewährt die Berechtigung zum Abrufen der Informationen eines Netzwerkprofils	Read	networkprofile*		
GetOfferingStatus	Gewährt die Berechtigung zum Abrufen des aktuellen und künftigen Status aller von einem AWS-Konto gekauften Angebote	Read			
GetProject	Gewährt die Berechtigung zum Abrufen von Informationen zu einem mobilen Testprojekt	Read	project*		
GetRemoteAccessSession	Gewährt die Berechtigung zum Abrufen des Links zu einer aktuell ausgeführten Remotezugriffssitzung	Read	session*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetRun	Gewährt die Berechtigung zum Abrufen der Informationen eines Laufs	Read	run*		
GetSuite	Gewährt die Berechtigung zum Abrufen der Informationen einer Testsuite	Read	suite*		
GetTest	Gewährt die Berechtigung zum Abrufen der Informationen eines Testfalls	Read	test*		
GetTestGridProject	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Desktop-Testprojekt	Read	testgrid-project*		
GetTestGridSession	Gewährt die Berechtigung zum Abrufen der Informationen einer Testrastersitzung	Read	testgrid-project		
			testgrid-session		
GetUpload	Gewährt die Berechtigung zum Abrufen der Informationen einer hochgeladenen Datei	Read	upload*		
GetVPCEConfiguration	Gewährt die Berechtigung zum Löschen einer Amazon Virtual Private Cloud (VPC)-Endpunktkonfiguration	Read	vpceconfiguration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
InstallToRemoteAccessSession	Gewährt die Berechtigung zum Installieren einer Anwendung auf einem Gerät in einer Remotezugriffssitzung	Write	session*		
			upload*		
ListArtifacts	Gewährt die Berechtigung zum Auflisten der Artefakte in einem Projekt	List	job		
			run		
			suite		
			test		
ListDeviceInstances	Gewährt die Berechtigung zum Auflisten der Informationen von Geräte-Instances	List			
ListDevicePools	Gewährt die Berechtigung zum Auflisten der Informationen von Gerätepools	List	project*		
ListDevices	Gewährt die Berechtigung zum Auflisten der Informationen eindeutiger Gerätetypen	List			
ListInstanceProfiles	Gewährt die Berechtigung zum Auflisten der Informationen von Geräte-Instance-Profilen	List			
ListJobs	Gewährt die Berechtigung zum Auflisten der Informationen von Aufträgen innerhalb eines Laufs	List	run*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListNetworkProfiles	Gewährt die Berechtigung zum Auflisten der Informationen von Netzwerkprofilen in einem Projekt	List	project*		
ListOfferingPromotions	Gewährt die Berechtigung zum Auflisten der Angebotsaktionen	List			
ListOfferingTransactions	Gewährt die Berechtigung zum Auflisten aller bisherigen Käufe, Erneuerungen und Systemerneuerungstransaktionen für ein AWS-Konto	List			
ListOfferings	Gewährt die Berechtigung zum Auflisten der Produkte oder Angebote, die der Benutzer über die API verwalten kann	List			
ListProjects	Gewährt die Berechtigung zum Auflisten der Informationen von mobilen Testprojekten für ein AWS-Konto	List			
ListRemoteAccessSessions	Gewährt die Berechtigung zum Auflisten der Informationen aktuell ausgeführter Remotezugriffssitzungen	List	project*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListRuns	Gewährt die Berechtigung zum Auflisten der Informationen von Ausführungen innerhalb eines Projekts	List	project*		
ListSamples	Gewährt die Berechtigung zum Auflisten der Informationen von Beispielen in einem Projekt	List	job*		
ListSuites	Gewährt die Berechtigung zum Auflisten der Informationen von Testsuites innerhalb eines Auftrags	List	job*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags einer Ressource	List	device		
			deviceinstance		
			devicepool		
			instanceprofile		
			networkprofile		
			project		
			run		
			session		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			testgrid-project		
			testgrid-session		
			vpceconfiguration		
ListTestGridProjects	Gewährt die Berechtigung zum Auflisten der Informationen von Desktop-Testprojekten für ein AWS-Konto	List			
ListTestGridSessionActions	Gewährt die Berechtigung zum Auflisten der während einer Testrastersitzung ausgeführten Sitzungsaktionen	List	testgrid-session*		
ListTestGridSessionArtifacts	Gewährt die Berechtigung zum Auflisten der von einer Testrastersitzung generierten Artefakte	List	testgrid-session*		
ListTestGridSessions	Gewährt die Berechtigung zum Auflisten der Sitzungen innerhalb eines Testrasterprojekts	List	testgrid-project*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTests	Gewährt die Berechtigung zum Auflisten der Informationen von Tests in einer Testsuite	List	suite*		
ListUniqueProblems	Gewährt die Berechtigung zum Auflisten von Informationen zu eindeutigen Problemen innerhalb einer Ausführung	List	run*		
ListUploads	Gewährt die Berechtigung zum Auflisten der Informationen von Uploads innerhalb eines Projekts	List	project*		
ListVPCEConfigurations	Gewährt die Berechtigung zum Löschen einer Amazon Virtual Private Cloud (VPC)-Endpunktkonfiguration	List			
PurchaseOffering	Gewährt die Berechtigung zum Kauf von Angeboten für ein AWS-Konto	Write			
RenewOffering	Gewährt die Berechtigung zum Festlegen der Anzahl der Geräte, die für ein Angebot verlängert werden sollen	Write			
ScheduleRun	Gewährt die Berechtigung zum Planen einer Ausführung	Write	project*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			devicepool		
			upload		
	SZENARIO: Device Pool as filter		devicepool* project* upload		
	SZENARIO: Device Selection Configuration as filter		project* upload		
StopJob	Gewährt die Berechtigung zum Beenden eines laufenden Auftrags	Write	job*		
StopRemoteAccessSession	Gewährt die Berechtigung zum Beenden einer laufenden Remotezugriffssitzung	Write	session*		
StopRun	Gewährt die Berechtigung zum Beenden eines laufenden Testlaufs	Write	run*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Ressource	Markieren	device		
			deviceinstance		
			devicepool		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			instanceprofile		
			networkprofile		
			project		
			run		
			session		
			testgrid-project		
			testgrid-session		
			vpceconfiguration		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Ressource	Markieren	device		
			deviceinstance		
			devicepool		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			instanceprofile		
			networkprofile		
			project		
			run		
			session		
			testgrid-project		
			testgrid-session		
			vpceconfiguration		
				aws:TagKeys	
UpdateDeviceInstance	Gewährt die Berechtigung zum Ändern einer vorhandenen Geräte-Instance	Write	deviceinstance*		
			instanceprofile		
UpdateDevicePool	Gewährt die Berechtigung zum Ändern eines vorhandenen Gerätepools	Write	devicepool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateInstanceProfile	Gewährt die Berechtigung zum Ändern eines vorhandenen Instance-Profils	Write	instanceprofile*		
UpdateNetworkProfile	Gewährt die Berechtigung zum Ändern eines vorhandenen Netzwerkprofils	Write	networkprofile*		
UpdateProject	Gewährt die Berechtigung zum, Ändern eines vorhandenen mobilen Testprojekts	Write	project*		ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateTestGridProject	Gewährt die Berechtigung zum Ändern eines vorhandenen Desktop-Testprojekts	Write	testgrid-project*		ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole
UpdateUpload	Gewährt die Berechtigung zum Ändern eines vorhandenen Uploads	Write	upload*		
UpdateVPCEConfiguration	Gewährt die Berechtigung zum Ändern einer Amazon Virtual Private Cloud (VPC)-Endpunktkonfiguration	Write	vpceconfiguration*		

Von AWS Device Farm definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden

können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
project	`arn:${Partition}:devicefarm:${Region}:${Account}:project:${ResourceId}`	aws:ResourceTag/${TagKey}
run	`arn:${Partition}:devicefarm:${Region}:${Account}:run:${ResourceId}`	aws:ResourceTag/${TagKey}
job	`arn:${Partition}:devicefarm:${Region}:${Account}:job:${ResourceId}`	
suite	`arn:${Partition}:devicefarm:${Region}:${Account}:suite:${ResourceId}`	
test	`arn:${Partition}:devicefarm:${Region}:${Account}:test:${ResourceId}`	
upload	`arn:${Partition}:devicefarm:${Region}:${Account}:upload:${ResourceId}`	
artifact	`arn:${Partition}:devicefarm:${Region}:${Account}:artifact:${ResourceId}`	
sample	`arn:${Partition}:devicefarm:${Region}:${Account}:sample:${ResourceId}`	
networkprofile	`arn:${Partition}:devicefarm:${Region}:${Account}:networkprofile:${ResourceId}`	aws:ResourceTag/${TagKey}
deviceinstance	`arn:${Partition}:devicefarm:${Region}::deviceinstance:${ResourceId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
session	`arn:${Partition}:devicefarm:${Region}:${Account}:session:${ResourceId}`	aws:ResourceTag/${TagKey}
devicepool	`arn:${Partition}:devicefarm:${Region}:${Account}:devicepool:${ResourceId}`	aws:ResourceTag/${TagKey}
device	`arn:${Partition}:devicefarm:${Region}::device:${ResourceId}`	aws:ResourceTag/${TagKey}
instanceprofile	`arn:${Partition}:devicefarm:${Region}:${Account}:instanceprofile:${ResourceId}`	aws:ResourceTag/${TagKey}
vpceconfiguration	`arn:${Partition}:devicefarm:${Region}:${Account}:vpceconfiguration:${ResourceId}`	aws:ResourceTag/${TagKey}
testgrid-project	`arn:${Partition}:devicefarm:${Region}:${Account}:testgrid-project:${ResourceId}`	aws:ResourceTag/${TagKey}
testgrid-session	`arn:${Partition}:devicefarm:${Region}:${Account}:testgrid-session:${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Device Farm

AWS Device Farm definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf den zulässigen Werten für die einzelnen Tags	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf dem Tag-Wert, der der Ressource zugeordnet ist	Zeichenfolge
aws:TagKeys	Filtert Aktionen basierend auf den obligatorischen Tags in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon DevOps Guru

Amazon DevOps Guru (Servicepräfix: `devops-guru`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon DevOps Guru definierte Aktionen
- Von Amazon DevOps Guru definierte Ressourcentypen
- Bedingungsschlüssel für Amazon DevOps Guru

Von Amazon DevOps Guru definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen.

Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddNotificationChannel	Gewährt die Berechtigung, einen Benachrichtigungskanal zu DevOps Guru hinzuzufügen	Schreiben	topic*		sns:GetTopicAttributes sns:SetTopicAttributes
DeleteInsight	Gewährt die Berechtigung zum Löschen bestimmter Erkenntnisse in Ihrem Konto	Schreiben			
DescribeAccountHealth	Gewährt die Berechtigung, den Zustand von Vorgängen in Ihrem AWS-Konto anzuzeigen	Read			
DescribeAccountOverview	Gewährt die Berechtigung, den Zustand von Vorgängen in Ihrem AWS-Konto innerhalb eines Zeitraums anzuzeigen	Read			
DescribeAnomaly	Gewährt die Berechtigung zum Auflisten der Details einer angegebenen Anomalie	Lesen			
DescribeEventSourcesConfig	Gewährt die Berechtigung zum Abrufen von Details zu Ereignisquellen für DevOps Guru	Lesen			
DescribeFeedback	Gewährt die Erlaubnis, die Feedback-Details einer	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	bestimmten Erkenntnis anzuzeigen				
DescribeInsight	Gewährt die Berechtigung zum Auflisten der Details einer angegebenen Erkenntnis	Lesen			
DescribeOrganizationHealth	Gewährt die Berechtigung, den Zustand von Operationen in Ihrer Organisation anzuzeigen	Lesen			
DescribeOrganizationOverview	Gewährt die Berechtigung, den Zustand von Operationen in Ihrer Organisation innerhalb eines Zeitraums anzuzeigen	Lesen			
DescribeOrganizationResourceCollectionHealth	Gewährt die Berechtigung zum Anzeigen des Zustands von Operationen für jeden AWS-CloudFormation-Stack oder für AWS-Services oder -Konten, die in DevOps Guru in Ihrer Organisation angegeben sind	Lesen			
DescribeResourceCollectionHealth	Gewährt die Berechtigung, für jeden in DevOps Guru angegebenen AWS CloudFormation-Stack den Status von Vorgängen anzuzeigen	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeServiceIntegration	Gewährt die Berechtigung, den Integrationsstatus von Services anzuzeigen, die in DevOps Guru integriert werden können	Read			
GetCostEstimation	Gewährt die Berechtigung zum Auflisten von Kostenschätzungen für Service-Ressourcen	Read			
GetResourceCollection	Gewährt die Berechtigung zum Auflisten von AWS CloudFormation-Stacks, für deren Verwendung DevOps Guru konfiguriert ist	Read			
ListAnomaliesForInsight	Gewährt die Berechtigung zum Auflisten von Anomalien einer bestimmten Erkenntnis in Ihrem Konto	Auflisten		devops-guru:ServiceNames	
ListAnomalousLogGroups	Gewährt die Berechtigung zum Auflisten von Anomalien einer bestimmten Erkenntnis in Ihrem Konto	Auflisten			
ListEvents	Gewährt die Berechtigung zum Auflisten von Ressourcenereignissen, die von DevOps Guru bewertet werden	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListInsights	Gewährt die Berechtigung zum Auflisten von Erkenntnissen in Ihrem Konto	Auflisten			
ListMonitoredResources	Gewährt die Berechtigung zum Auflisten der von DevOps Guru verwalteten Ressourcen in Ihrem Konto	Auflisten			
ListNotificationChannels	Gewährt die Berechtigung zum Auflisten von Benachrichtigungskanälen, die in Ihrem Konto für DevOps Guru konfiguriert sind	Auflisten			
ListOrganizationInsights	Gewährt die Berechtigung zum Auflisten von Erkenntnissen in Ihrer Organisation	Auflisten			
ListRecommendations	Gewährt die Berechtigung zum Auflisten der Empfehlungen einer angegebenen Erkenntnis	List			
PutFeedback	Gewährt die Berechtigung, Feedback an DevOps Guru zu übermitteln	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RemoveNotificationChannel	Gewährt die Berechtigung, einen Benachrichtigungskanal aus DevOps Guru zu entfernen	Write	topic*		sns:GetTopicAttributes sns:SetTopicAttributes
SearchInsights	Gewährt die Berechtigung zum Suchen von Erkenntnissen in Ihrem Konto	Auflisten		devops-guru:ServiceNames	
SearchOrganizationInsights	Gewährt die Berechtigung zum Suchen von Erkenntnissen in Ihrer Organisation	Auflisten			
StartCostEstimation	Gewährt die Erlaubnis, mit der Erstellung einer Schätzung der monatlichen Kosten zu beginnen	Lesen			
UpdateEventSourcesConfig	Gewährt die Berechtigung zum Aktualisieren einer Ereignisquelle für DevOps Guru	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateResourceCollection	Gewährt die Berechtigung zum Aktualisieren der Liste von AWS CloudFormation-Stacks, mit denen angegeben wird, welche AWS-Ressourcen in Ihrem Konto von DevOps Guru analysiert werden	Schreiben			
UpdateServiceIntegration	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren eines in DevOps Guru integrierten Services	Schreiben			

Von Amazon DevOps Guru definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
topic	`arn:${Partition}:sns:${Region}:${Account}:${TopicName}`	

Bedingungsschlüssel für Amazon DevOps Guru

Amazon DevOps Guru definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
devops-guru:ServiceNames	Filtert den Zugriff per API, um den Zugriff auf bestimmte AWS-Servicenamen einzuschränken	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Diagnosetools

AWS Diagnosetools (Servicepräfix: `ts`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Diagnosetools definierte Aktionen
- Von AWS Diagnosetools definierte Ressourcentypen
- Zustandsschlüssel für AWS Diagnosetools

Von AWS Diagnosetools definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetExecution	Gewährt die Berechtigung zum Abrufen von Details zu bestimmten Ausführungen in AWS Diagnosetools	Lesen	execution*		
GetExecutionOutput	Gewährt die Berechtigung zum Abrufen von Details zu bestimmten Ausführungsausgaben in AWS Diagnosetools	Lesen	execution*		
GetTool	Gewährt die Berechtigung zum Abrufen von Details zu bestimmten Tools in AWS Diagnosetools	Lesen	tool*		
ListExecutions	Gewährt die Berechtigung, alle verfügbaren Ausführungen in AWS Diagnosetools aufzulisten	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für eine AWS Diagnosetools-Ressource.	Lesen	execution*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTools	Gewährt die Berechtigung, alle verfügbaren Tools in AWS Diagnosetools aufzulisten	Auflisten			
StartExecution	Gewährt die Berechtigung, einen Ausführungsworkflow für ein bestimmtes Tool in den AWS Diagnosetools zu starten	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
TagResource	Gewährt die Berechtigung zum Markieren einer AWS Diagnosetool-Ressource	Markierung	execution*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer AWS Diagnosetool-Ressource	Markierung	execution*		
				aws:TagKeys	

Von AWS Diagnosetools definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
execution	`arn:${Partition}:ts::${Account}:execution/${UserId}/${ToolId}/${ExecutionId}`	aws:ResourceTag/${TagKey}
tool	`arn:${Partition}:ts::aws:tool/${ToolId}`	

Zustandsschlüssel für AWS Diagnosetools

AWS Diagnosetools definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den zulässigen Werten für jeden der Tags	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Tag-Wert, der der Ressource zugeordnet ist	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach dem Vorhandensein verbindlicher Tags in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Direct Connect

AWS Direct Connect (Servicepräfix: `directconnect`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Direct Connect definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptDirectConnectGatewayAssociationProposal	Gewährt die Berechtigung, eine Anforderung für einen Vorschlag zum Anfügen eines Virtual Private Gateways an ein Direct-Connect-Gateway anzunehmen	Schreiben	dx-gateway*		
AllocateConnectionOnInterconnect	Gewährt die Berechtigung zum Erstellen einer gehosteten Verbindung über eine Interconnect-Verbindung	Schreiben	dxcon*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AllocateHostedConnection	Gewährt die Berechtigung zum Erstellen einer neuen gehosteten Verbindung zwischen dem Netzwerk eines AWS-Direct-Connect-Partners und einem bestimmten AWS-Direct-Connect-Standort	Schreiben	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
AllocatePrivateVirtualInterface	Gewährt die Berechtigung zum Bereitstellen einer privaten virtuellen Schnittstelle, deren Eigentümer ein anderer Kunde sein soll	Schreiben	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
AllocatePublicVirtualInterface	Gewährt die Berechtigung zum Bereitstellen einer öffentlichen virtuellen Schnittstelle, deren Eigentümer ein anderer Kunde sein soll	Schreiben	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AllocateTransitVirtualInterface	Gewährt die Berechtigung zum Bereitstellen einer virtuellen Transit-Schnittstelle, deren Eigentümer ein anderer Kunde sein soll	Schreiben	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociateConnectionWithLag	Gewährt die Berechtigung zum Zuordnen einer Verbindung mit einer Link-Aggregationsgruppe (LAG)	Schreiben	dxcon*		
			dxlag*		
AssociateHostedConnection	Gewährt die Berechtigung zum Zuordnen einer gehostete Verbindung und deren virtuelle Schnittstellen mit einer Link-Aggregationsgruppe (LAG) oder einer Interconnect-Verbindung	Schreiben	dxcon*		
			dxcon		
			dxlag		
AssociateMacSecKey	Gewährt die Berechtigung zum Zuordnen eines MAC-Sicherheit (MACsec)-Verbindungsschlüsselnamens (CKN) /Connectivity Association Key (CAK)-Paares mit einer AWS zugehörige Direct-Connect-Verbindung	Schreiben	dxcon		
			dxlag		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateVirtualInterface	Gewährt die Berechtigung zum Zuordnen einer virtuellen Schnittstelle mit einer angegebenen Link-Aggregationsgruppe (LAG) oder einer Verbindung	Schreiben	dxvif*		
			dxcon		
			dxlag		
ConfirmConnection	Gewährt die Berechtigung, die Erstellung einer gehosteten Verbindung über eine Interconnect-Verbindung zu bestätigen	Schreiben	dxcon*		
ConfirmCustomerAgreement	Gewährt die Berechtigung zur Bestätigung der Vertragsbedingungen beim Erstellen der Verbindung oder der Link-Aggregationsgruppe (LAG)	Schreiben			
ConfirmPrivateVirtualInterface	Gewährt die Berechtigung, den Eigentum an einer von einem anderen Kunden erstellten privaten virtuellen Schnittstelle anzunehmen	Schreiben	dxvif*		
ConfirmPublicVirtualInterface	Gewährt die Berechtigung, den Eigentum an einer von einem anderen Kunden erstellten öffentlichen virtuellen Schnittstelle anzunehmen	Schreiben	dxvif*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ConfirmTransitVirtualInterface	Gewährt die Berechtigung, den Eigentum an einer von einem anderen Kunden erstellten virtuellen Transit-Schnittstelle anzunehmen	Schreiben	dxvif*		
CreateBGPPeer	Gewährt die Berechtigung zum Erstellen eines BGP-Peers für die angegebene virtuelle Schnittstelle	Schreiben	dxvif*		
CreateConnection	Gewährt die Berechtigung zu Erstellen einer neuen Verbindung zwischen dem Kundennetzwerk und einem bestimmten AWS-Direct-Connect-Standort	Schreiben	dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDirectConnectGateway	Gewährt die Berechtigung zum Erstellen eines Direct-Connect-Gateways als Zwischenobjekt, mit dem Sie eine Verbindung mit einer Reihe von virtuellen Schnittstellen und Virtual Private Gateways herstellen können	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDirectConnectGatewayAssociation	Gewährt die Berechtigung zu Erstellen einer Zuordnung zwischen einem Direct-Connect-Gateway und einem Virtual Private Gateway	Schreiben	dx-gateway*		
CreateDirectConnectGatewayAssociationProposal	Gewährt die Berechtigung zum Erstellen eines Vorschlags zur Zuordnung des angegebenen Virtual Private Gateway mit dem angegebenen Direct-Connect-Gateway	Schreiben	dx-gateway*		
CreateInterconnect	Gewährt die Berechtigung zum Erstellen einer neuen Interconnect-Verbindung zwischen dem Netzwerk eines AWS-Direct-Connect-Partners und einem bestimmten AWS-Direct-Connect-Standort	Schreiben	dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLag	Gewährt die Berechtigung zum Erstellen einer Link-Aggregationsgruppe (LAG) mit der angegebenen Anzahl von gebündelten physischen Verbindungen zwischen dem Kundennetzwerk und einem bestimmten AWS-Direct-Connect-Standort	Schreiben	dxcon		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreatePrivateVirtualInterface	Gewährt die Berechtigung zum Erstellen einer neuen privaten virtuellen Schnittstelle	Schreiben	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePublicVirtualInterface	Gewährt die Berechtigung zum Erstellen einer neuen öffentlichen virtuellen Schnittstelle	Schreiben	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTransitVirtualInterface	Gewährt die Berechtigung zum Erstellen einer neuen virtuellen Transit-Schnittstelle	Schreiben	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteBGPPeer	Gewährt die Berechtigung zum Löschen des angegebenen BGP-Peers in der angegebenen virtuellen Schnittstelle mit der angegebenen Kundenadresse und dem ASN	Schreiben	dxvif*		
DeleteConnection	Gewährt die Berechtigung zum Löschen der Verbindung	Schreiben	dxcon*		
DeleteDirectConnectGateway	Gewährt die Berechtigung zum Löschen des angegebenen Direct-Connect-Gateways	Schreiben	dx-gateway*		
DeleteDirectConnectGatewayAssociation	Gewährt die Berechtigung zum Löschen der Zuordnung zwischen dem angegebenen Direct-Connect-Gateway und einem Virtual Private Gateway	Schreiben	dx-gateway*		
DeleteDirectConnectGatewayAssociationProposal	Gewährt die Berechtigung zum Löschen der Anforderung für einen Zuordnungs-Vorschlag zwischen dem angegebenen Direct-Connect-Gateway und einem Virtual Private Gateway	Schreiben			
DeleteInterconnect	Gewährt die Berechtigung zum Löschen der angegebenen Interconnect-Verbindung	Schreiben	dxcon*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteLag	Gewährt die Berechtigung zum Löschen der angegebenen Link-Aggregationsgruppe (LAG)	Schreiben	dxlag*		
DeleteVirtualInterface	Gewährt die Berechtigung zum Löschen einer virtuellen Schnittstelle	Schreiben	dxvif*		
DescribeConnectionLoa	Gewährt die Berechtigung, die LOA-CFA für eine Verbindung zu beschreiben	Lesen	dxcon*		
DescribeConnections	Gewährt die Berechtigung zum Beschreiben aller Verbindungen in dieser Region	Lesen	dxcon		
DescribeConnectionsOnInterconnect	Gewährt die Berechtigung, eine Liste von Verbindungen zu beschreiben, die über die gegebene Interconnect-Verbindung bereitgestellt wurden	Lesen	dxcon*		
DescribeCustomerMetadata	Gewährt die Berechtigung, eine Liste der Kundenvereinbarungen sowie deren unterschriebenen Status anzuzeigen und ob der Kunde ein NNIPartner, NNIPartnerV2 oder ein nonPartner ist	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDirectConnectGatewayAssociationProposals	Gewährt die Berechtigung zum Beschreiben einer oder mehrere Zuordnungs-Vorschläge für die Verbindung zwischen einem Virtual Private Gateway und einem Direct-Connect-Gateway	Lesen	dx-gateway		
DescribeDirectConnectGatewayAssociations	Gewährt die Berechtigung zum Beschreiben der Zuordnungen zwischen Ihren Direct-Connect-Gateways und Virtual Private Gateways	Lesen	dx-gateway		
DescribeDirectConnectGatewayAttachments	Gewährt die Berechtigung zum Beschreiben der Anhänge zwischen Ihren Direct-Connect-Gateways und virtuellen Schnittstellen	Lesen	dx-gateway		
DescribeDirectConnectGateways	Gewährt die Berechtigung zum Beschreiben aller Ihrer Direct-Connect-Gateways oder nur des angegebenen Direct-Connect-Gateways	Lesen	dx-gateway		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeHostedConnections	Gewährt die Berechtigung zum Beschreiben der gehosteten Verbindungen, die auf der angegebenen Interconnect-Verbindung oder Link-Aggregationsgruppe (LAG) bereitgestellt wurden	Lesen	dxcon		
			dxlag		
DescribeInterconnectLoa	Gewährt die Berechtigung, die LOA-CFA für eine Interconnect-Verbindung zu beschreiben	Lesen	dxcon*		
DescribeInterconnects	Gewährt die Berechtigung zum Beschreiben einer Liste der Interconnect-Verbindungen, die im Besitz des AWS-Konto sind	Lesen	dxcon		
DescribeLags	Gewährt die Berechtigung zum Beschreiben aller Ihrer Link-Aggregationsgruppe (LAG) oder der angegebenen LAG	Lesen	dxlag		
DescribeLoa	Gewährt die Berechtigung zum Beschreiben des LOA-CFA für eine Verbindung, Interconnect-Verbindung oder Link-Aggregationsgruppe (LAG)	Lesen	dxcon		
			dxlag		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeLocations	Gewährt die Berechtigung zum Beschreiben der Liste von AWS-Direct-Connect-Standorten in der aktuellen AWS-Region	Lesen			
DescribeRouterConfiguration	Gewährt die Berechtigung, Details zum Router für eine virtuelle Schnittstelle zu beschreiben	Lesen	dxvif*		
DescribeTags	Gewährt die Berechtigung zum Beschreiben der Tags, die den angegebenen AWS-Direct Connect-Ressourcen zugeordnet sind	Lesen	dxcon		
			dxlag		
			dxvif		
DescribeVirtualGateways	Gewährt die Berechtigung zum Beschreiben einer Liste der Virtual Private Gateways, die im Besitz des AWS-Konto sind	Lesen			
DescribeVirtualInterfaces	Gewährt die Berechtigung zum Beschreiben aller virtuellen Schnittstellen für ein AWS-Konto	Lesen	dxcon		
			dxlag		
			dxvif		
DisassociateConnectionFromLag	Gewährt die Berechtigung zum Trennen einer Verbindung mit einer Link-Aggregationsgruppe (LAG)	Schreiben	dxcon*		
			dxlag*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateMacSecKey	Gewährt die Berechtigung zum Entfernen der Verknüpfung zwischen einem MAC-Sicherheitsschlüssel (MacSec-Sicherheitsschlüssel) und einer AWSzugehörige Direct-Connect-Verbindung	Schreiben	dxcon		
			dxlag		
ListVirtualInterfaceTestHistory	Gewährt die Berechtigung zum Auflisten des Failover-Testverlaufs der virtuellen Schnittstelle	Auflisten	dxvif*		
StartBgpFailoverTest	Gewährt die Berechtigung zum Starten des Failover-Tests der virtuellen Schnittstelle, der überprüft, ob Ihre Konfiguration Ihre Ausfallsicherheits-Anforderungen erfüllt, indem die BGP-Peering-Sitzung in den DOWN-Zustand versetzt wird. Anschließend können Sie Datenverkehr senden, um sicherzustellen, dass keine Ausfälle vorliegen	Schreiben	dxvif*		
StopBgpFailoverTest	Gewährt die Berechtigung zum Beenden des Failover-Tests der virtuellen Schnittstelle	Schreiben	dxvif*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Hinzufügen der angegebenen Tags zur angegebenen AWS-Direct-Connect-Ressource. Jede Ressource kann maximal 50 Tags haben	Markierung	dxcon		
			dxlag		
			dxvif		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen eines oder mehrerer Tags aus der angegebenen AWS-Direct-Connect-Ressource	Markierung	dxcon		
			dxlag		
			dxvif		
				aws:TagKeys	
UpdateConnection	Gewährt die Berechtigung zum Aktualisieren desAWSDirect Connect dedizierte Verbindungskonfiguration Sie können die folgenden Parameter für eine Verbindung aktualisieren: Der Verbindungsname oder der MAC-Sicherheits-Verschlüsselungsmodus (MAC Security) der Verbindung	Schreiben	dxcon*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateDirectConnectGateway	Gewährt die Berechtigung zum Aktualisieren des Namens eines Direct-Connect-Gateways	Schreiben	dx-gateway*		
UpdateDirectConnectGatewayAssociation	Gewährt die Berechtigung zum Aktualisieren der angegebenen Attribute der Direct-Connect-Gateway-Zuordnung	Schreiben			
UpdateLag	Gewährt die Berechtigung zum Aktualisieren der Attribute der angegebenen Link Aggregation Group (LAG)	Schreiben	dxlag*		
UpdateVirtualInterfaceAttributes	Gewährt die Berechtigung zum Aktualisieren der angegebenen Attribute der angegebenen virtuellen privaten Schnittstelle	Schreiben	dxvif*		

Von AWS Direct Connect definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
dxcon	`arn:${Partition}:directconnect:${Region}:${Account}:dxcon/${ConnectionId}`	aws:ResourceTag/${TagKey}
dxlag	`arn:${Partition}:directconnect:${Region}:${Account}:dxlag/${LagId}`	aws:ResourceTag/${TagKey}
dxvif	`arn:${Partition}:directconnect:${Region}:${Account}:dxvif/${VirtualInterfaceId}`	aws:ResourceTag/${TagKey}
dx-gateway	`arn:${Partition}:directconnect::${Account}:dx-gateway/${DirectConnectGatewayId}`	

Bedingungsschlüssel für AWS Direct Connect

AWS Direct Connect definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff danach, ob Tag-Schlüssel-Wert-Paare in der Anforderung vorhanden sind	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tag-Schlüssel-Wert-Paaren, die der Ressource angefügt sind	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert Zugriff basierend auf dem Vorhandensein von Tag-Schlüsseln in der Anforderung	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Directory Service

AWS Directory Service (Servicepräfix: `ds`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Directory Service definierte Aktionen
- Von AWS Directory Service definierte Ressourcentypen
- Bedingungsschlüssel für AWS Directory Service

Von AWS Directory Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung

mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptSharedDirectory	Gewährt die Berechtigung zum Annehmen einer Verzeichnisfreigabeanforderung, die vom Konto des Verzeichniseigentümers gesendet wurde	Schreiben	directory*		
AddIpRoutes	Gewährt die Berechtigung zum Hinzufügen eines CIDR-	Schreiben	directory*		ec2:AuthorizeSecur

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Adressblocks für die korrekte Weiterleitung des Datenverkehrs zu und von Ihrem Microsoft AD in Amazon Web Services				ityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:DescribeSecurityGroups

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddRegion	Gewährt die Berechtigung zum Hinzufügen von zwei Domain-Controllern in der angegebenen Region für das angegebene Verzeichnis	Schreiben	directory*		ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddTagsToResource	Gewährt die Berechtigung zum Hinzufügen oder Überschreiben von einem oder mehreren Tags für das angegebene Amazon-Directory-Service-Verzeichnis	Markierung	directory*		ec2:CreateTags
				aws:RequestTag/${TagKey} aws:TagKeys	
AuthorizeApplication [nur Berechtigung]	Gewährt die Berechtigung zur Autorisierung einer Anwendung für Ihr AWS-Verzeichnis	Schreiben	directory*		
CancelSchemaExtension	Gewährt die Berechtigung zum Abbrechen einer laufenden Schemaerweiterung auf ein Microsoft-AD-Verzeichnis	Schreiben	directory*		
CheckAlias [nur Berechtigung]	Gewährt die Berechtigung zum Überprüfen, ob der Alias zur Verwendung verfügbar ist	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ConnectDirectory	Gewährt die Berechtigung zum Erstellen eines AD Connectors zum Verbinden mit einem On-Premises-Verzeichnis	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAlias	Gewährt die Berechtigung zum Erstellen einen Alias für ein Verzeichnis und weist den Alias dem Verzeichnis zu	Schreiben	directory*		
CreateComputer	Gewährt die Berechtigung zum Erstellen eines Computerkontos im angegebenen Verzeichnis und verknüpft den Computer mit dem Verzeichnis	Schreiben	directory*		
CreateConditionalForwarder	Gewährt die Berechtigung zum Erstellen einer bedingten Weiterleitung, die Ihrem AWS-Verzeichnis zugeordnet ist	Schreiben	directory*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDirectory	Gewährt die Berechtigung zum Erstellen eines Simple AD-Verzeichnisses	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateIdentityPoolDirectory [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines IdentityPool-Verzeichnisses in der AWS Cloud	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLogSubscription	Gewährt die Berechtigung zum Erstellen eines Abonnements zur Weiterleitung von Echtzeit-Sicherheitsprotokollen des Directory-Service-Domain-Controllers an die angegebene CloudWatch-Protokollgruppe in Ihrem AWS-Konto	Schreiben	directory*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateMicrosoftAD	Gewährt die Berechtigung zum Erstellen eines Microsoft AD in der AWS Cloud	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSnapshot	Gewährt die Berechtigung zum Erstellen eines Snapshots eines Simple AD- oder Microsoft AD-Verzeichnisses in der AWS Cloud	Schreiben	directory*		
CreateTrust	Gewährt die Berechtigung zum Initiieren der Erstellung der AWS-Seite einer Vertrauensstellung zwischen einem Microsoft AD in der AWS Cloud und einer externen Domain	Schreiben	directory*		
DeleteConditionalForwarder	Gewährt die Berechtigung zum Löschen einer bedingten Weiterleitung, die für Ihr AWS-Verzeichnis eingerichtet wurde.	Schreiben	directory*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteDirectory	Gewährt die Berechtigung zum Löschen eines AWS-Directory-Service-Verzeichnisses	Schreiben	directory*		ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup ec2:DescribeNetworkInterfaces ec2:RevokeSecurityGroupEgress ec2:RevokeSecurityGroupIngress
DeleteLogSubscription	Gewährt die Berechtigung zum Löschen der angegebenen Protokollabonnements	Schreiben	directory*		
DeleteSnapshot	Gewährt die Berechtigung zum Löschen eines Verzeichnis-Snapshots	Schreiben	directory*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteTrust	Gewährt die Berechtigung zum Löschen einer bestehenden Vertrauensstellung zwischen Ihrem Microsoft AD in der AWS Cloud und einer externen Domain	Schreiben	directory*		
DeregisterCertificate	Gewährt die Berechtigung zum Löschen des Zertifikats, das für eine gesicherte LDAP-Verbindung registriert wurde, aus dem System	Schreiben	directory*		
DeregisterEventTopic	Gewährt die Berechtigung zum Entfernen des angegebenen Verzeichnisses als Publisher für das angegebene SNS-Thema	Schreiben	directory*		
DescribeCertificate	Gewährt die Berechtigung zum Anzeigen von Informationen über das Zertifikat, das für eine gesicherte LDAP-Verbindung registriert ist	Lesen	directory*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeClientAuthenticationSettings	Gewährt die Berechtigung zum Abrufen von Informationen über den Typ der Clientauthentifizierung für das angegebene Verzeichnis, wenn der Typ angegeben ist. Wenn kein Typ angegeben ist, werden Informationen zu allen Client-Authentifizierungstypen abgerufen, die für das angegebene Verzeichnis unterstützt werden. Derzeit wird nur SmartCard unterstützt.	Lesen	directory*		
DescribeConditionalForwarders	Gewährt die Berechtigung zum Erhalten von Informationen über die bedingten Weiterleitungen für dieses Konto	Lesen	directory*		
DescribeDirectories	Gewährt die Berechtigung zum Erhalten von Informationen über die Verzeichnisse, die zu diesem Konto gehören	Auflisten			
DescribeDomainControllers	Gewährt die Berechtigung zum Bereitstellen von Informationen über Domain-Controller in Ihrem Verzeichnis	Lesen	directory*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeEventTopics	Gewährt die Berechtigung zum Erhalten von Informationen darüber, welche SNS-Themen Statusmeldungen vom angegebenen Verzeichnis erhalten	Lesen	directory*		
DescribeLDAPSSettings	Gewährt die Berechtigung zum Beschreiben des Status der LDAP-Sicherheit für das angegebene Verzeichnis	Lesen	directory*		
DescribeRegions	Gewährt die Berechtigung zum Bereitstellen von Informationen zu den Regionen, die für multiregionale Replikation konfiguriert sind	Lesen	directory*		
DescribeSettings	Erteilt die Berechtigung zum Abrufen von Informationen zu den konfigurierbaren Einstellungen für das angegebene Verzeichnis.	Lesen	directory*		
DescribeSharedDirectories	Gewährt die Berechtigung zum Zurückgeben der freigegebenen Verzeichnisse in Ihrem Konto	Lesen	directory*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeSnapshots	Gewährt die Berechtigung zum Erhalten von Informationen über die Verzeichnis-Snapshots, die zu diesem Konto gehören	Lesen			
DescribeTrusts	Gewährt die Berechtigung zum Erhalten von Informationen über die Vertrauensstellungen für dieses Konto	Lesen			
DescribeUpdateDirectory	Gewährt die Berechtigung zum Beschreiben der Aktualisierungen eines Verzeichnisses für einen bestimmten Aktualisierungstyp	Lesen	directory*		
DisableClientAuthentication	Gewährt die Berechtigung zum Deaktivieren alternativer Client-Authentifizierungsmethoden für das angegebene Verzeichnis	Schreiben	directory*		
DisableLDAPS	Gewährt die Berechtigung zum Deaktivieren sicherer LDAP-Aufrufe für das angegebene Verzeichnis	Schreiben	directory*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisableRadius	Gewährt die Berechtigung zum Deaktivieren von Multi-Faktor-Authentifizierung (MFA) mit dem Server des Remote Authentication Dial In User Service (RADIUS) für ein AD-Connector-Verzeichnis	Schreiben	directory*		
DisableRoleAccess [nur Berechtigung]	Gewährt die Berechtigung zum Deaktivieren des AWS Management Console-Zugriffs auf Identitäten in Ihrem AWS-Verzeichnis	Schreiben	directory*		
DisableSso	Gewährt die Berechtigung zum Deaktivieren von Single-Sign-On für ein Verzeichnis	Schreiben	directory*		
EnableClientAuthentication	Gewährt die Berechtigung zum Aktivieren alternativer Client-Authentifizierungsmethoden für das angegebene Verzeichnis	Schreiben	directory*		
EnableLDAPS	Gewährt die Berechtigung zum Aktivieren des Switches für das angegebene Verzeichnis, um immer sichere LDAP-Aufrufe zu verwenden	Schreiben	directory*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
EnableRadius	Gewährt die Berechtigung zum Aktivieren von Multi-Faktor-Authentifizierung (MFA) mit dem Server des Remote Authentication Dial In User Service (RADIUS) für ein AD-Connector-Verzeichnis	Schreiben	directory*		
EnableRoleAccess [nur Berechtigung]	Gewährt die Berechtigung zum Aktivieren des AWS Management Console-Zugriffs auf Identitäten in Ihrem AWS-Verzeichnis	Schreiben	directory*		iam:PassRole
EnableSso	Gewährt die Berechtigung zum Aktivieren von Single-Sign-On für ein Verzeichnis	Schreiben	directory*		
GetAuthorizedApplicationDetails [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen der Details der autorisierten Anwendungen in einem Verzeichnis	Lesen	directory*		
GetDirectoryLimits	Gewährt die Berechtigung zum Erhalten von Informationen über das Verzeichnislimit für die aktuelle Region	Lesen			
GetSnapshotLimits	Gewährt die Berechtigung zum Erhalten des manuellen Snapshot-Limits für ein Verzeichnis	Lesen	directory*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAuthorizedApplications [nur Berechtigung]	Gewährt die Berechtigung zum Erhalten der AWS-Anwendungen, die für ein Verzeichnis autorisiert sind	Lesen	directory*		
ListCertificates	Gewährt die Berechtigung, alle Zertifikate, die für eine gesicherte LDAP-Verbindung registriert sind, für das angegebene Verzeichnis aufzulisten	Auflisten	directory*		
ListIpRoutes	Gewährt die Berechtigung zum Auflisten der Adressblöcke, die Sie einem Verzeichnis hinzugefügt haben	Lesen	directory*		
ListLogSubscriptions	Gewährt die Berechtigung zum Auflisten der aktiven Protokollabonnements für das AWS-Konto	Lesen			
ListSchemaExtensions	Gewährt die Berechtigung zum Auflisten aller Schemaerweiterungen, die auf ein Microsoft AD-Verzeichnis angewendet wurden	Auflisten	directory*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten aller Tags für ein Amazon-Directory-Service-Verzeichnis	Lesen	directory*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RegisterCertificate	Gewährt die Berechtigung zum Registrieren eines Zertifikats für eine gesicherte LDAP-Verbindung	Schreiben	directory*		
RegisterEventTopic	Gewährt die Berechtigung zum Verknüpfen eines Verzeichnisses mit einem SNS-Thema	Schreiben	directory*		sns:GetTopicAttributes
RejectSharedDirectory	Gewährt die Berechtigung zum Ablehnen einer Verzeichnisfreigabeanforderung, die vom Konto des Verzeichniseigentümers gesendet wurde	Schreiben	directory*		
RemoveIpRoutes	Gewährt die Berechtigung zum Entfernen von IP-Adressblöcken aus einem Verzeichnis	Schreiben	directory*		
RemoveRegion	Gewährt die Berechtigung zum Stoppen der gesamten Replikation und entfernt die Domain-Controller aus der angegebenen Region Sie können mit diesem Vorgang die primäre Region nicht entfernen.	Schreiben	directory*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RemoveTagsFromResource	Gewährt die Berechtigung zum Entfernen von Tags aus einem Amazon-Directory-Service-Verzeichnis	Markierung	directory*		ec2:DeleteTags
				aws:RequestTag/${TagKey} aws:TagKeys	
ResetUserPassword	Gewährt die Berechtigung zum Zurücksetzen des Passworts für Benutzer in Ihrem von AWS verwalteten Microsoft AD- oder Simple AD-Verzeichnis	Schreiben	directory*		
RestoreFromSnapshot	Gewährt die Berechtigung zum Wiederherstellen eines Verzeichnisses mithilfe eines vorhandenen Verzeichnis-Snapshots	Schreiben	directory*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ShareDirectory	Gewährt die Berechtigung zum Freigeben eines angegebenen Verzeichnisses in Ihrem AWS-Konto (Verzeichnisbesitzer) für ein anderes AWS-Konto (Verzeichnisverbraucher). Für diesen Vorgang können Sie Ihr Verzeichnis aus einem beliebigen AWS-Konto und aus einer beliebigen Amazon VPC innerhalb einer AWS-Region verwenden.	Schreiben	directory*		
StartSchemaExtension	Gewährt die Berechtigung zum Anwenden einer Schemaerweiterung auf ein Microsoft AD-Verzeichnis	Schreiben	directory*		
UnauthorizeApplication [nur Berechtigung]	Gewährt die Berechtigung zum Aufheben der Autorisierung einer Anwendung für Ihr AWS-Verzeichnis	Schreiben	directory*		
UnshareDirectory	Gewährt die Berechtigung zum Stoppen der Verzeichnisfreigabe zwischen den Konten des Verzeichnisbesitzers und -verbrauchers	Schreiben	directory*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateAuthorizedApplication [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren einer autorisierten Anwendung für Ihr AWS-Verzeichnis	Schreiben	directory*		
UpdateConditionalForwarder	Gewährt die Berechtigung zum Aktualisieren einer bedingten Weiterleitung, die für Ihr AWS-Verzeichnis eingerichtet wurde	Schreiben	directory*		
UpdateDirectory [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren der Konfigurationen wie Servicekontoanmeldeinformationen oder DNS-Server-IP-Adressen für das angegebene Verzeichnis	Schreiben	directory*		
UpdateDirectorySetup	Gewährt die Berechtigung zum Aktualisieren des Verzeichnisses für einen bestimmten Aktualisierungstyp	Schreiben	directory*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateNumberOfDomainControllers	Gewährt die Berechtigung zum Hinzufügen oder Entfernen von Domain-Controllern zu bzw. aus dem Verzeichnis Basierend auf dem Unterschied zwischen dem aktuellen Wert und dem neuen Wert (der durch diesen API-Aufruf bereitgestellt wird), werden Domain-Controller hinzugefügt oder entfernt. Es kann bis zu 45 Minuten dauern, bis neue Domain-Controller vollständig aktiv werden, nachdem die angeforderte Anzahl von Domain-Controllern aktualisiert wurde. Während dieser Zeit können Sie keine andere Aktualisierungsanforderung durchführen.	Schreiben	directory*		
UpdateRadius	Gewährt die Berechtigung zum Aktualisieren der Serverinformationen des Remote Authentication Dial In User Service (RADIUS) für ein AD-Connector-Verzeichnis	Schreiben	directory*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateSettings	Gewährt die Berechtigung zum Aktualisieren der Beendigungseinstellungen für den angegebenen Voice Connector.	Schreiben	directory*		
UpdateTrust	Gewährt die Berechtigung zum Aktualisieren der Vertrauensstellung, die zwischen Ihrem von AWS verwalteten Microsoft AD-Verzeichnis und einem On-Premises Active Directory eingerichtet wurde	Schreiben	directory*		
VerifyTrust	Gewährt die Berechtigung zum Verifizieren einer Vertrauensstellung zwischen Ihrem Microsoft AD in der AWS Cloud und einer externen Domain	Lesen	directory*		

Von AWS Directory Service definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
directory	`arn:${Partition}:ds:${Region}:${Account}:directory/${DirectoryId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Directory Service

AWS Directory Service definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Wert der Anforderung an AWS DS	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach der AWS-DS-Ressource, für die Maßnahmen ergriffen werden	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon DocumentDB Elastic Clusters

Amazon DocumentDB Elastic Clusters (Service-Präfix: `docdb-elastic`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon DocumentDB Elastic Clusters definierte Aktionen
- Von Amazon DocumentDB Elastic Clusters definierte Ressourcentypen
- Bedingungsschlüssel für Amazon DocumentDB Elastic Clusters

Von Amazon DocumentDB Elastic Clusters definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CopyClusterSnapshot	Erteilt die Erlaubnis, einen neuen Amazon DoCDB-Elastic Cluster-Snapshot zu kopieren	Schreiben	cluster-snapshot*		docdb-elastic:CreateClusterSnapshot kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey
				aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCluster	Gewährt die Berechtigung zum Erstellen eines neuen Amazon-DocDB-Elastic-Cluster	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ec2:ModifyVpcEndpoint iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy secretsmanager:Get

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					SecretValue secretsmanager:ListSecretVersionIds secretsmanager:ListSecrets

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateClusterSnapshot	Gewährt die Berechtigung zum Erstellen eines neuen Amazon-DocDB-Elastic-Cluster-Snapshots	Schreiben	cluster*		ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ec2:ModifyVpcEndpoint iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy secretsmanager:Get

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					SecretValue secretsmanager:ListSecretVersionIds secretsmanager:ListSecrets
			cluster-snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteCluster	Gewährt die Berechtigung zum Löschen eines Clusters	Schreiben	cluster*		ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteClusterSnapshot	Gewährt die Berechtigung zum Löschen eines Cluster-Snapshots	Schreiben	cluster-snapshot*		ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
GetCluster	Gewährt die Berechtigung zum Anzeigen von Details zu einem Cluster	Lesen	cluster*		
				aws:ResourceTag/${TagKey}	
GetClusterSnapshot	Gewährt die Berechtigung zum Abrufen von Details über einen Cluster-Snapshot	Lesen	cluster-snapshot*		
				aws:ResourceTag/${TagKey}	
ListClusterSnapshots	Gewährt die Berechtigung zum Auflisten der Cluster-Snapshots in Ihrem Konto	Auflisten			
ListClusters	Gewährt die Berechtigung zum Auflisten der Cluster in Ihrem Konto	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine DocumentDB-Elastic-Ressource	Auflisten	cluster		
			cluster-snapshot		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RestoreClusterFromSnapshot	Gewährt die Berechtigung zum erneuten Erstellen eines neuen Amazon-DocDB-Elastic-Cluster-Snapshots	Schreiben	cluster*		docdb-elastic:CreateCluster ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ec2:DescribeVpcs ec2:ModifyVpcEndpoint iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					secretsmanager:GetSecretValue secretsmanager:ListSecretVersionIds secretsmanager:ListSecrets
			cluster-snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
StartCluster	Erteilt die Erlaubnis, einen gestoppten Amazon DoCDB-Elastic-Cluster zu starten	Schreiben	cluster*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopCluster	Erteilt die Erlaubnis, einen vorhandenen Amazon DoCDB-Elastic-Cluster zu beenden	Schreiben	cluster*		
				aws:ResourceTag/${TagKey}	
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer DocumentDB-Elastic-Ressource	Tagging	cluster		
			cluster-snapshot		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
				aws:ResourceTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags zu einer DocumentDB-Elastic-Ressource	Tagging	cluster		
			cluster-snapshot		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateCluster	Gewährt die Berechtigung zum Ändern eines Clusters	Schreiben	cluster*		ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ec2:ModifyVpcEndpoint kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy secretsmanager:GetSecretValue secretsmanager:Lis

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					tSecretVersionIds secretsmanager:ListSecrets
				aws:ResourceTag/${TagKey}	

Von Amazon DocumentDB Elastic Clusters definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
cluster	`arn:${Partition}:docdb-elastic:${Region}:${Account}:cluster/${ResourceId}`	aws:ResourceTag/${TagKey}
cluster-snapshot	`arn:${Partition}:docdb-elastic:${Region}:${Account}:cluster-snapshot/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon DocumentDB Elastic Clusters

Amazon DocumentDB Elastic Cluster definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Satz von Tag-Schlüssel-Wert-Paaren in der Anforderung	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert den Zugriff nach dem Satz von Tag-Schlüsseln in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon DynamoDB

Amazon DynamoDB (Servicepräfix: `dynamodb`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon DynamoDB definierte Aktionen

- Von Amazon DynamoDB definierte Ressourcentypen
- Bedingungsschlüssel für Amazon DynamoDB

Von Amazon DynamoDB definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetItem	Gewährt die Berechtigung, die Attribute einzelner oder mehrerer Elemente aus einzelnen oder mehreren Tabellen zurückzugeben	Lesen	table*		
				dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:Select	
BatchWriteItem	Gewährt die Berechtigung zum Ablegen oder Löschen mehrerer Elemente aus einzelnen oder mehreren Tabellen	Schreiben	table*		
				dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity	
ConditionCheckItem	Gewährt die Berechtigung für die - ConditionCheckItem	Lesen	table*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Operation überprüft das Vorhandensein einer Reihe von Attributen für das Element mit dem angegebenen Primärschlüssel			dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
CreateBackup	Gewährt die Berechtigung zum Erstellen eines Backups für eine vorhandene Tabelle	Schreiben	table*		
CreateGlobalTable	Gewährt die Berechtigung zum Erstellen einer globalen Tabelle aus einer vorhandene Tabelle	Schreiben	global-table* table*		
CreateTable	Gewährt die Berechtigung für die - CreateTable Operation fügt Ihrem Konto eine neue Tabelle hinzu	Schreiben	table*		
CreateTableReplica [nur Berechtigung]	Gewährt die Berechtigung zum Hinzufügen einer neuen Replikattabelle	Schreiben	table*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteBackup	Gewährt die Berechtigung zum Löschen eines vorhandenen Backups für eine Tabelle	Schreiben	backup*		
DeleteItem	Gewährt die Berechtigung zum Löschen eines einzelnen Elements in einer Tabelle nach Primärschlüssel	Schreiben	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
DeleteResourcePolicy	Gewährt die Berechtigung zum Löschen der ressourcenbasierten Richtlinie, die der Ressource zugeordnet ist	Berechtigungsverwaltung	stream*		
			table*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteTable	Gewährt die Berechtigung für den DeleteTable Vorgang, der eine Tabelle und alle zugehörigen Elemente löscht	Schreiben	table*		
DeleteTableReplica [nur Berechtigung]	Gewährt die Berechtigung zum Löschen einer Replikattabelle und aller zugehörigen Elemente	Schreiben	table*		
DescribeBackup	Gewährt die Berechtigung zum Beschreiben eines vorhandenen Backups für eine Tabelle	Lesen	backup*		
DescribeContinuousBackups	Gewährt die Berechtigung, den Status der Einstellungen für Sicherung und Wiederherstellung für die angegebene Tabelle zu überprüfen	Lesen	table*		
DescribeContributorInsights	Gewährt die Berechtigung zum Beschreiben des Contributor-Insights-Status und die zugehörigen Details für eine bestimmte Tabelle oder einen globalen sekundären Index	Lesen	table* index		
DescribeEndpoints	Gewährt die Berechtigung zum Zurückgeben der regionalen Endpunktinformationen	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeExport	Gewährt die Berechtigung zum Beschreiben eines vorhandenen Exports für eine Tabelle	Lesen	export*		
DescribeGlobalTable	Gewährt die Berechtigung zum Zurückgeben von Informationen zur angegebenen globalen Tabelle	Lesen	global-table*		
DescribeGlobalTableSettings	Gewährt die Berechtigung zum Zurückgeben von Einstellungs-Informationen zur angegebenen globalen Tabelle	Lesen	global-table*		
DescribeImport	Gewährt die Berechtigung zum Beschreiben eines bestehenden Imports.	Lesen	import*		
DescribeKinesisStreamingDestination	Gewährt die Berechtigung, den Status des Kinesis-Streamings und verwandter Details für eine bestimmte Tabelle zu beschreiben	Lesen	table*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeLimits	Gewährt die Berechtigung, die aktuellen bereitgestellten Kapazitätsgrenzen für Ihr AWS-Konto in einer Region zurückzugeben, sowohl für die Region als auch für jede einzelne DynamoDB-Tabelle, die Sie dort erstellen	Lesen			
DescribeReservedCapacity [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben einer oder mehrere der erworbenen reservierten Kapazität	Lesen			
DescribeReservedCapacityOfferings [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben der Angebote für reservierte Kapazität, die zum Kauf verfügbar sind	Lesen			
DescribeStream	Gewährt die Berechtigung, Informationen über einen Stream zurückzugeben, inklusive des aktuellen Status des Streams, seinen Amazon-Ressourcennamen (ARN), die Zusammenstellung der Shards und die zugehörige DynamoDB-Tabelle	Lesen	stream*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeTable	Gewährt die Berechtigung zum Zurückgeben von Informationen zur Tabelle	Lesen	table*		
DescribeTableReplicaAutoScaling	Gewährt die Berechtigung zum Beschreiben der Auto-Scaling-Einstellungen in allen Replikaten der globalen Tabelle	Lesen	table*		
DescribeTimeToLive	Gewährt die Berechtigung, den Status der Time to Live (TTL, Gültigkeitsdauer) für die angegebene Tabelle zu beschreiben	Lesen	table*		
DisableKinesisStreamingDestination	Gewährt die Berechtigung zum Beenden der Replikation von der DynamoDB-Tabelle auf den Kinesis-Datenstream	Schreiben	table*		
EnableKinesisStreamingDestination	Gewährt die Berechtigung, die Tabellendatenreplikation auf den angegebenen Kinesis-Datenstream bei einem Zeitstempel zu starten, der während der Aktivierung des Workflows gewählt wurde	Schreiben	table*		
ExportTableToPointInTime	Gewährt die Berechtigung zum Initiieren eines Exports einer DynamoDB-Tabelle nach S3	Schreiben	table*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetItem	Gewährt die Berechtigung für die GetItem Operation, die einen Satz von Attributen für das Element mit dem angegebenen Primärschlüssel zurückgibt	Lesen	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:Select	
GetRecords	Gewährt die Berechtigung zum Abruffen der Stream-Datensätze aus einem gegebenen Shard	Lesen	stream*		
GetResourcePolicy	Gewährt die Berechtigung zum Anzeigen einer ressourcenbasierten Richtlinie für eine Ressource	Lesen	stream*		
			table*		
GetShardIterator	Gewährt die Berechtigung zum Zurückgeben eines Shard-Iterators	Lesen	stream*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ImportTable	Gewährt die Berechtigung zum Initiieren eines Imports von S3 zu einer DynamoDB-Tabelle.	Schreiben	table*		
ListBackups	Gewährt die Berechtigung zum Auflisten von Backups, die dem Konto und dem Endpunkt zugeordnet sind	Auflisten			
ListContributorInsights	Gewährt die Berechtigung zum Auflisten der ContributorInsightsSummary für alle Tabellen und globalen sekundären Indizes, die dem aktuellen Konto und Endpunkt zugeordnet sind	Auflisten			
ListExports	Gewährt die Berechtigung zum Auflisten von Exporten, die dem Konto und dem Endpunkt zugeordnet sind	Auflisten			
ListGlobalTables	Gewährt die Berechtigung zum Auflisten aller globalen Tabellen, die in der angegebenen Region ein Replikat haben	Auflisten			
ListImports	Gewährt die Berechtigung zum Auflisten von Importen, die dem Konto und dem Endpunkt zugeordnet sind.	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListStreams	Gewährt die Berechtigung, ein Array der Stream-ARNs zurückzugeben, die dem aktuellen Konto und Endpunkt zugeordnet sind	Lesen			
ListTables	Gewährt die Berechtigung, ein Array der Tabellen-Namen zurückzugeben, die dem aktuellen Konto und Endpunkt zugeordnet sind	Auflisten			
ListTagsOfResource	Gewährt die Berechtigung zum Auflisten aller Tags auf einer Amazon-DynamoDB-Ressource	Lesen	table*		
PartiQLDelete	Gewährt die Berechtigung zum Löschen eines einzelnen Elements in einer Tabelle nach Primärschlüssel	Write	table*	dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnValues	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PartiQLInsert	Gewährt die Berechtigung zum Erstellen eines neuen Elements, sofern kein Element mit demselben Primärschlüssel in der Tabelle vorhanden ist	Write	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys	
PartiQLSelect	Gewährt die Berechtigung zum Lesen einer Reihe von Attributen für Elemente aus einer Tabelle oder einem Index	Read	table*		
			index		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:FullTableScan dynamodb:LeadingKeys dynamodb:Select	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PartiQLUpdate	Gewährt die Berechtigung zum Bearbeiten der Attribute eines vorhandenen Elements	Schreiben	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnValues	
PurchaseReservedCapacityOfferings [nur Berechtigung]	Gewährt die Berechtigung zum Kauf von reservierter Kapazität zur Verwendung mit dem Konto	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutItem	Gewährt die Berechtigung, ein neues Element zu erstellen oder ein altes durch ein neues Element zu ersetzen	Schreiben	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
PutResourcePolicy	Gewährt die Berechtigung zum Anfügen einer ressourcenbasierten Richtlinie an die Ressource	Berechtigungsverwaltung	stream*		
			table*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Query	Gewährt die Berechtigung, den Primärschlüssel einer Tabelle oder einen sekundären Index für den direkten Zugriff auf Elemente in der Tabelle bzw. im Index zu verwenden	Lesen	table*		
			index		
				dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues dynamodb:Select	
RestoreTableFromAwsBackup [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer neuen Tabelle vom Wiederherstellungspunkt auf AWS Backup	Schreiben	table*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RestoreTableFromBackup	Gewährt die Berechtigung zum Erstellen einer neuen Tabelle aus einem vorhandenen Backup	Schreiben	backup*		dynamodb:BatchWriteItem dynamodb:DeleteItem dynamodb:GetItem dynamodb:PutItem dynamodb:Query dynamodb:Scan dynamodb:UpdateItem
			table*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RestoreTableToPointInTime	Gewährt die Berechtigung zum Wiederherstellen einer Tabelle zu einem beliebigen Zeitpunkt	Schreiben	table*		dynamodb:BatchWriteItem dynamodb:DeleteItem dynamodb:GetItem dynamodb:PutItem dynamodb:Query dynamodb:Scan dynamodb:UpdateItem

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Scan	Gewährt die Berechtigung, einzelne oder mehrere Elemente und Elementattribute zurückzugeben, indem auf jedes Element in einer Tabelle oder einen sekundären Index zugegriffen wird	Lesen	table*		
			index		
				dynamodb:Attributes dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues dynamodb:Select	
StartAwsBackupJob [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines Backups auf AWS Backup mit aktivierten erweiterten Funktionen	Schreiben	table*		
TagResource	Gewährt die Berechtigung zum Verknüpfen einer Gruppe von Tags mit einer Amazon-DynamoDB-Ressource	Tagging	table*		
UntagResource	Gewährt die Berechtigung zum Entfernen der Zuordnungen von Tags zu einer Amazon-DynamoDB-Ressource	Tagging	table*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateContinuousBackups	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren von kontinuierlichen Backups	Schreiben	table*		
UpdateContributorInsights	Gewährt die Berechtigung, den Status für Contributor Insights für eine bestimmte Tabelle oder einen globalen Sekundärindex zu aktualisieren	Schreiben	table* index		
UpdateGlobalTable	Gewährt die Berechtigung zum Hinzufügen oder Entfernen von Replikaten aus der angegebenen globalen Tabelle	Schreiben	global-table* table*		
UpdateGlobalTableSettings	Gewährt die Berechtigung zum Aktualisieren der angegebenen globalen Tabelle	Schreiben	global-table* table*		
UpdateGlobalTableVersion [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren der angegebenen globalen Tabelle	Schreiben	global-table* table		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateItem	Gewährt die Berechtigung zum Bearbeiten der Attribute eines vorhandenen Elements oder zum hinzufügen eines neuen Elements in die Tabelle, wenn es noch nicht existiert	Schreiben	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
UpdateKinesisStreamingDestination	Gewährt die Berechtigung zum Aktualisieren von Datenreplikationskonfigurationen für den angegebenen Kinesis-Datenstrom	Schreiben	table*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateTable	Gewährt die Berechtigung, die bereitgestellten Durchsatzeinstellungen, globalen sekundären Indizes oder DynamoDB-Streams-Einstellungen für eine gegebene Tabelle zu ändern	Schreiben	table*		
UpdateTableReplicaAutoScaling	Gewährt die Berechtigung zum Aktualisieren der Auto-Scaling-Einstellungen in der Replikattabelle	Schreiben	table*		
UpdateTimeToLive	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren von TTL für die angegebene Tabelle	Schreiben	table*		

Von Amazon DynamoDB definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressource ntypen	ARN	Bedingungsschlüssel
index	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/index/${IndexName}`	
stream	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/stream/${StreamLabel}`	
table	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}`	
backup	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/backup/${BackupName}`	
export	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/export/${ExportName}`	
global-table	`arn:${Partition}:dynamodb::${Account}:global-table/${GlobalTableName}`	
import	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/import/${ImportName}`	

Bedingungsschlüssel für Amazon DynamoDB

Amazon DynamoDB definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

> **Note**
>
> Informationen zur Verwendung von Kontextschlüsseln für die Optimierung des DynamoDB-Zugriffs mithilfe einer IAM-Richtlinie finden Sie unter Verwenden von IAM-Richtlinienbedingungen für die differenzierte Zugriffskontrolle im Amazon DynamoDB-Entwicklerhandbuch.

Bedingungsschlüssel	Beschreibung	Typ
dynamodb:Attributes	Filtert den Zugriff basiert auf Attributnamen (Feld- oder Spaltennamen) der Tabelle	ArrayOfString
dynamodb:EnclosingOperation	Filtert den Zugriff durch Blockieren von Aufrufen durch Transaktions-APIs, Durchlassen von Aufrufen durch Nicht-Transaktions-APIs und umgekehrt	String
dynamodb:FullTableScan	Filtert den Zugriff durch Blockieren des vollständigen Tabellenscans	Bool
dynamodb:LeadingKeys	Filtert den Zugriff durch den Partitionsschlüssel der Tabelle	ArrayOfString
dynamodb:ReturnConsumedCapacity	Filtert den Zugriff nach dem ReturnConsumedCapacity Parameter einer Anforderung. Enthält entweder „TOTAL“ oder „NONE“	String
dynamodb:ReturnValues	Filtert den Zugriff nach dem ReturnValues Parameter der Anforderung. Enthält eine der folgenden Optionen: „ALL_OLD“, „UPDATED_OLD“, „ALL_NEW“, „UPDATED_NEW“ oder „NONE“	String
dynamodb:Select	Filtert den Zugriff durch den Select-Parameter einer Abfrage- oder Scan-Anforderung	String

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon DynamoDB Accelerator (DAX)

Amazon DynamoDB Accelerator (DAX) (Service-Präfix: `dax`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon DynamoDB Accelerator (DAX) definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie

den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetItem	Gewährt die Berechtigung, die Attribute einzelner oder mehrerer Elemente aus einzelnen oder mehreren Tabellen zurückzugeben	Lesen	application*		
BatchWriteItem	Gewährt die Berechtigung zum Ablegen oder Löschen mehrerer Elemente aus einzelnen oder mehreren Tabellen	Schreiben	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ConditionCheckItem	Gewährt die Berechtigung für die ConditionCheckItem-Operation, die das Vorhandensein einer Reihe von Attributen für das Element mit dem angegebenen Primärschlüssel überprüft	Lesen	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCluster	Gewährt die Berechtigung zum Erstellen eines DAX-Clusters	Schreiben	application*		dax:CreateParameterGroup dax:CreateSubnetGroup ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:GetRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					iam:PassRole
CreateParameterGroup	Gewährt die Berechtigung zum Erstellen einer Parametergruppe	Schreiben			
CreateSubnetGroup	Gewährt die Berechtigung zum Erstellen einer Subnetzgruppe	Schreiben			
DecreaseReplicationFactor	Gewährt die Berechtigung zum Entfernen eines oder mehrerer Knoten aus einem DAX-Cluster	Schreiben	application*		
DeleteCluster	Gewährt die Berechtigung zum Löschen eines zuvor bereitgestellten DAX-Clusters	Schreiben	application*		
DeleteItem	Gewährt die Berechtigung zum Löschen eines einzelnen Elements in einer Tabelle nach Primärschlüssel	Schreiben	application*		
				dax:EnclosingOperation	
DeleteParameterGroup	Gewährt die Berechtigung zum Löschen der angegebenen Parametergruppe	Schreiben			
DeleteSubnetGroup	Gewährt die Berechtigung zum Löschen einer Subnetzgruppe	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeClusters	Gewährt die Berechtigung zum zurückgeben von Informationen über alle bereitgestellten DAX-Cluster	Auflisten	application		
DescribeDefaultParameters	Gewährt die Berechtigung, die Standard-System-Parameterinformationen für DAX zurückzugeben	Auflisten			
DescribeEvents	Gewährt die Berechtigung zum Zurückgeben von Ereignissen im Zusammenhang mit DAX-Clustern und Parametergruppen	Auflisten			
DescribeParameterGroups	Gewährt die Berechtigung zum Zurückgeben einer Liste von Parametergruppenbeschreibungen	Auflisten			
DescribeParameters	Gewährt die Berechtigung zum Zurückgeben der detaillierten Parameterliste für eine bestimmte Parametergruppe	Lesen			
DescribeSubnetGroups	Gewährt die Berechtigung zum Zurückgeben einer Liste von Subnetzgruppenbeschreibungen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetItem	Gewährt der Produktion GetItem-Operation die Berechtigung, einen Satz von Attributen für das Element mit dem gegebenen Primärschlüssel zurückzugeben	Lesen	application*		
				dax:EnclosingOperation	
IncreaseReplicationFactor	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Knoten zu einem DAX-Cluster	Schreiben	application*		
ListTags	Gewährt die Berechtigung zum Zurückgeben einer Liste aller Tags für einen DAX-Cluster	Lesen	application*		
PutItem	Gewährt die Berechtigung, ein neues Element zu erstellen oder ein altes durch ein neues Element zu ersetzen	Schreiben	application*		
				dax:EnclosingOperation	
Query	Gewährt die Berechtigung, den Primärschlüssel einer Tabelle oder einen sekundären Index für den direkten Zugriff auf Elemente in der Tabelle bzw. im Index zu verwenden	Lesen	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RebootNode	Gewährt die Berechtigung zum erneuten Starten eines einzelnen Knotens eines DAX-Clusters	Schreiben	application*		
Scan	Gewährt die Berechtigung, einzelne oder mehrere Elemente und Elementattribute zurückzugeben, indem auf jedes Element in einer Tabelle oder einen sekundären Index zugegriffen wird	Lesen	application*		
TagResource	Gewährt die Berechtigung zum Zuordnen einer Reihe von Tags zu einer DAX-Ressource	Markierung	application*		
UntagResource	Gewährt die Berechtigung zum Entfernen der Zuordnungen von Tags aus einer DAX-Ressource	Markierung	application*		
UpdateCluster	Gewährt die Berechtigung zum Ändern der Einstellungen für einen DAX-Cluster	Schreiben	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateItem	Gewährt die Berechtigung zum Bearbeiten der Attribute eines vorhandenen Elements oder zum hinzufügen eines neuen Elements in die Tabelle, wenn es noch nicht existiert	Schreiben	application*		
				dax:EnclosingOperation	
UpdateParameterGroup	Gewährt die Berechtigung zum Ändern der Parameter einer Parametergruppe	Schreiben			
UpdateSubnetGroup	Gewährt die Berechtigung zum Ändern einer vorhanden en Subnetzgruppe	Schreiben			

Vom Amazon DynamoDB Accelerator (DAX) definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
application	`arn:${Partition}:dax:${Region}:${Account}:cache/${ClusterName}`	

Bedingungsschlüssel für Amazon DynamoDB Accelerator (DAX)

Amazon DynamoDB Accelerator (DAX) definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
dax:EnclosingOperation	Wird verwendet, um Aufrufe durch Transaktions-APIs zu blockieren und Aufrufe durch Nicht-Transaktions-APIs durchzulassen und umgekehrt	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2

Amazon EC2 (Servicepräfix: `ec2`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon EC2 definierte Aktionen
- Von Amazon EC2 definierte Ressourcentypen
- Bedingungsschlüssel für Amazon EC2

Von Amazon EC2 definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptAddressTransfer	Gewährt die Berechtigung zum Akzeptieren einer Elastic-IP-Adressen-Übertragung	Schreiben	elastic-ip*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AllocationId ec2:Domain ec2:PubliclpAddress	ec2:CreateTags
				ec2:Region	
AcceptReservedInstancesExchangeQuote	Gewährt die Berechtigung, ein Convertible Reserved Instance-Austauschangebot zu akzeptieren	Write		ec2:Region	
AcceptTransitGatewayMulticastDomainAssociations	Gewährt die Berechtigung, eine Anforderung zum Zuordnen von Subnetzen zu einer Transit-Gateway-Multicast-Domain zu akzeptieren	Write	transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:transitGatewayAttachmentId	
			transit-gateway-multicast-domain	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	
AcceptTransitGatewayPeeringAttachment	Gewährt die Berechtigung zum Annehmen einer Transit-Gateway-Peering-Anlagenanforderung	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
AcceptTransitGatewayVpcAttachment	Gewährt die Berechtigung, eine Anforderung zum Zuordnen einer VPC zu einem Transit-Gateway anzunehmen	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	
AcceptVpcEndpointConnections	Gewährt die Berechtigung, eine oder mehrere Schnittstellen-VPC-Endpunktverbindungen mit Ihrem VPC-Endpunkt-Service zu akzeptieren	Write	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptVpcPeeringConnection	Gewährt die Berechtigung zum Annehmen einer VPC-Peering-Verbindungsanforderung	Schreiben	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
			vpc-peering-connection*	aws:ResourceTag/${TagKey} ec2:AccepterVpc ec2:RequesterVpc ec2:ResourceTag/${TagKey} ec2:VpcPeeringConnectionID	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AdvertiseByoipCidr	Erteilt die Erlaubnis, für einen IP-Adressbereich zu werben, der für die Verwendung AWS über Bring Your Own IP Addresses (BYOIP) bereitgestellt wurde	Schreiben		ec2:Region	
AllocateAddress	Gewährt die Berechtigung, Ihrem Konto eine Elastic IP-Adresse (EIP) zuzuweisen	Write	elastic-ip*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			ipv4pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AllocateHosts	Gewährt die Berechtigung, Ihrem Konto einen Dedicated Host zuzuweisen	Schreiben	dedicated-host*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AutoPlacement ec2:AvailabilityZone ec2:HostRecovery ec2:InstanceType ec2:Quantity	ec2:CreateTags
				ec2:Region	
AllocateIpamPoolCidr	Gewährt die Berechtigung, ein CIDR aus einem Amazon VPC IP Address Manager (IPAM)-Pool zuzuweisen	Schreiben	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
ApplySecurityGroupsToClientVpnTargetNetwork	Gewährt die Berechtigung, eine Sicherheitsgruppe auf die Mapping zwischen einem Client-VPN-Endpunkt und einem Zielnetzwerk anzuwenden	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssignIpv6Addresses	Gewährt die Berechtigung zum Zuweisen einer oder mehrerer IPv6-Adressen zu einer Netzwerkschnittstelle	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssignPrivateIpAddresses	Gewährt die Berechtigung, eine oder mehrere sekundäre private IP-Adressen einer Netzwerkschnittstelle zuzuweisen	Schreiben	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	
AssignPrivateNatGatewayAddress	Gewährt die Berechtigung zum Zuweisen von einer oder mehreren sekundären privaten IP-Adressen zu einem NAT-Gateway	Schreiben	natgateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateAddress	Gewährt die Berechtigung, eine Elastic IP-Adresse (EIP) mit einer Instance oder einer Netzwerkschnittstelle zu verknüpfen	Write	elastic-ip	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PubliclpAddress ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			instance	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateClientVpnTargetNetwork	Gewährt die Berechtigung, ein Zielnetzwerk mit einem Client-VPN-Endpunkt zu verknüpfen	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			subnet*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SubnetID	
				ec2:Region	
Associate DhcpOptions	Gewährt die Berechtigung, eine Gruppe von DHCP-Optionen einer VPC zuzuordnen oder ihre Mapping aufzuheben	Write	dhcp-options*	aws:ResourceTag/${TagKey} ec2:DhcpOptionsID ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
AssociateEnclaveCertificateIamRole	Gewährt die Berechtigung, ein ACM-Zertifikat einer IAM-Rolle zuzuordnen, um sie in einer EC2-Enclave zu verwenden	Write	certificate*		
			role*		
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateIamInstanceProfile	Gewährt die Berechtigung, ein IAM-Instance-Profil einer ausgeführten oder gestoppten Instance zuzuordnen	Schreiben	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:NewInstanceProfile ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
AssociateInstanceEventWindow	Gewährt die Berechtigung zum Zuweisen eines oder mehrerer Ziele zu einem Ereignisfenster	Schreiben	instance-event-window*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
AssociateIpamByoasn	Gewährt die Berechtigung, einer BYOIP CIDR eine Autonome Systemnummer (ASN) zuzuordnen	Schreiben		ec2:Region	
AssociateIpamResourceDiscovery	Erteilt die Erlaubnis, eine IPAM-Ressourcenerkennung mit einem Amazon VPC IPAM zu verknüpfen	Schreiben	ipam*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			ipam-resource-discovery*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			ipam-resource-discovery-association*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	
AssociateNatGatewayAddress	Gewährt die Berechtigung zum Zuordnen einer Elastic-IP-Adresse und privaten IP-Adresse zu einem öffentlichen NAT-Gateway	Schreiben	elastic-ip*	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			natgateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
Associate RouteTable	Gewährt die Berechtigung, ein Subnetz oder ein Gateway mit einer Routing-Tabelle zu verknüpfen	Write	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			internet-gateway	aws:ResourceTag/${TagKey} ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			vpn-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
AssociateSubnetCidrBlock	Gewährt die Berechtigung, einen CIDR-Block einem Subnetz zuzuordnen	Write	subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
AssociateTransitGatewayMulticastDomain	Gewährt die Berechtigung, eine Anlage und Liste von Subnetzen zu einer Transit-Gateway-Multicast-Domain zuzuordnen	Schreiben	subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			transit-gateway-multicast-domain*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateTransitGatewayPolicyTable	Erteilung der Erlaubnis, eine Richtlinientabelle mit einem Transit-Gateway-Anhang zu verknüpfen	Schreiben	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			transit-gateway-policy-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayPolicyTableId	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateTransitGatewayRouteTable	Gewährt die Berechtigung zum Zuordnen einer Anlage zu einer Transit-Gateway-Routing-Tabelle	Schreiben	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
				ec2:Region	
AssociateTrunkInterface	Gewährt die Berechtigung, eine Zweignetzwerkschnittstelle mit einer Trunk-Netzwerkschnittstelle	Schreiben		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateVerifiedAccessInstanceWebAcl [nur Berechtigung]	Erteilt die Berechtigung, einer AWS Verified Access-Instanz eine Web Application Firewall (WAF) Web Access Control List (ACL) zuzuordnen	Schreiben	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
AssociateVpcCidrBlock	Gewährt die Berechtigung zum Verknüpfen eines CIDR-Blocks mit einer VPC	Schreiben	vpc*	aws:ResourceTag/${TagKey} ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			ipv6pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AttachClassicLinkVpc	Erteilt die Berechtigung, eine EC2-Classic-Instance über eine oder mehrere Sicherheitsgruppen der VPC mit einer ClassicLink -fähigen VPC zu verknüpfen	Schreiben	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AttachInternetGateway	Gewährt die Berechtigung zum Anfügen eines Internet-Gateways an eine VPC	Write	internet-gateway*	aws:ResourceTag/${TagKey} ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AttachNetworkInterface	Gewährt die Berechtigung zum Zuordnen einer Netzwerkschnittstelle zu einer Instance	Schreiben	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	
AttachVerifiedAccessTrustProvider	Gewährt die Berechtigung zum Anhängen eines Vertrauensanbieters zu einer Instance mit verifiziertem Zugriff	Schreiben	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			verified-access-trust-provider*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AttachVolume	Gewährt die Berechtigung, ein EBS-Volume an eine ausgeführte oder gestoppte Instance anzufügen und es der Instance mit dem angegebenen Gerätenamen zur Verfügung zu stellen.	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:Encrypted ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
AttachVpnGateway	Gewährt die Berechtigung zum Zuordnen eines Virtual Private Gateways zu einer VPC	Write	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
			vpn-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AuthorizeClientVpnIngress	Gewährt die Berechtigung zum Hinzufügen einer Autorisierungsregel für eingehenden Datenverkehr zu einem Client-VPN-Endpunkt	Schreiben	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AuthorizeSecurityGroupEgress	Gewährt die Berechtigung zum Hinzufügen einer oder mehrerer ausgehender Regeln zu einer VPC-Sicherheitsgruppe. Richtlinien, die die Berechtigung auf security-group-rule Ressourcenebene verwenden, werden nur durchgesetzt, wenn die API-Anfrage Folgendes beinhaltet TagSpecifications	Schreiben	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	ec2:CreateTags
			security-group-rule	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AuthorizeSecurityGroupIngress	Gewährt die Berechtigung zum Hinzufügen einer oder mehrerer Regeln für eingehenden Datenverkehr zu einer VPC-Sicherheitsgruppe. Richtlinien, die die Berechtigung security-group-rule auf Ressourcenebene verwenden, werden nur durchgesetzt, wenn die API-Anfrage Folgendes umfasst TagSpecifications	Schreiben	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	ec2:CreateTags
			security-group-rule	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	
BundleInstance	Gewährt die Berechtigung zum Bündeln einer durch Instance-Speicher gestützten Windows-Instance	Write		ec2:Region	
CancelBundleTask	Gewährt die Berechtigung zum Abbrechen eines Bündelvorgangs	Write		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelCapacityReservation	Gewährt die Berechtigung, eine Kapazitätsreservierung zu stornieren und die reservierte Kapazität freizugeben	Schreiben	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:CapacityReservationFleet ec2:ResourceTag/${TagKey}	
				ec2:Region	
CancelCapacityReservationFleets	Gewährt die Erlaubnis, eine oder mehrere Flotten mit Kapazitätsreservierung zu stornieren	Schreiben	capacity-reservation-fleet*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CancelCapacityReservation
				ec2:Region	
CancelConversionTask	Gewährt die Berechtigung zum Abbrechen einer aktiven Konvertierungsaufgabe	Write		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelExportTask	Gewährt die Berechtigung zum Abbrechen einer aktiven Exportaufgabe	Schreiben	export-image-task	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			export-instance-task	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelImageLaunchPermission	Erteilt die Erlaubnis, Ihre AWS-Konto Startberechtigungen für das angegebene AMI zu entfernen	Schreiben	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	
CancelImportTask	Gewährt die Berechtigung, eine laufende Aufgabe zum Importieren einer virtuellen Maschine oder zum Importieren eines Snapshots zu stornieren	Write	import-image-task	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			import-snapshot-task	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CancelReservedInstancesListing	Gewährt die Berechtigung zum Stornieren eines Reserved Instance-Angebots auf dem Reserved Instance Marketplace	Write		ec2:Region	
CancelSpotFleetRequests	Gewährt die Berechtigung zum Stornieren einer oder mehrerer Spot-Flottenanforderungen	Write	spot-fleet-request*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelSpotInstanceRequests	Gewährt die Berechtigung zum Stornieren einer oder mehrerer Spot-Instance-Anforderungen	Write	spot-instances-request*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ConfirmProductInstance	Gewährt die Berechtigung, zu bestimmen, ob ein eigener Produktcode einer Instance zugeordnet ist	Write		ec2:Region	
CopyFpgaImage	Gewährt die Berechtigung, ein Quell-AFI (Amazon FPGA-Image) in die aktuelle Region zu kopieren. Die für diese Aktion angegebenen Berechtigungen auf Ressourcenebene gelten nur für das neue AFI. Sie gelten nicht für die Quell-AFI	Write	fpga-image*	ec2:Owner	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CopyImage	Gewährt die Berechtigung, ein Amazon Machine Image (AMI) aus einer Quellregion in die aktuelle Region zu kopieren. Die für diese Aktion angegebenen Berechtigungen auf Ressourcenebene gelten nur für das neue AMI. Sie gelten nicht für das Quell-AMI	Schreiben	image*	aws:RequestTag/${TagKey} aws:TagKeys ec2:ImageID ec2:Owner	ec2:CreateTags
				ec2:Region	
CopySnapshot	Erteilt die Erlaubnis, einen point-in-time Snapshot eines EBS-Volumes zu kopieren und in Amazon S3 zu speichern. Die für diese Aktion angegebenen Berechtigungen auf Ressourcenebene gelten nur für den neue Snapshot. Sie gelten nicht für den Quell-Snapshot	Write	snapshot*	aws:RequestTag/${TagKey} aws:TagKeys ec2:OutpostArn ec2:SnapshotID	ec2:CreateTags
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCapacityReservation	Gewährt die Berechtigung zum Erstellen einer Kapazitätsreservierung	Schreiben	capacity-reservation*	aws:RequestTag/${TagKey} aws:TagKeys ec2:CapacityReservationFleet	ec2:CreateTags
				ec2:Region	
CreateCapacityReservationFleet	Gewährt die Berechtigung zum Erstellen einer Kapazitätsreservierungsflotte	Schreiben	capacity-reservation-fleet*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateCapacityReservation ec2:CreateTags ec2:DescribeCapacityReservations ec2:DescribeInstances
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCarrierGateway	Gewährt die Berechtigung zum Erstellen eines Carrier-Gateways und stellt VPC-Kunden CSP-Konnektivität bereit.	Write	carrier-gateway*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateClientVpnEndpoint	Gewährt die Berechtigung zum Erstellen eines Client-VPN-Endpunkts	Write	client-vpn-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:SamlProviderArn ec2:ServerCertificateArn	ec2:CreateTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID	
			vpc	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpcID	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateClientVpnRoute	Gewährt die Berechtigung zum Hinzufügen einer Netzwerkroute zur Routing-Tabelle eines Client-VPN-Endpunkts	Schreiben	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			subnet*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SubnetID	
				ec2:Region	
CreateCoipCidr	Erteilt die Berechtigung zum Erstellen eines Bereichs von IP-Adressen (CoIP) im Besitz des Kunden	Schreiben	coip-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateCoipPool	Erteilt die Berechtigung zum Erstellen eines Pools von IP-Adressen (CoIP) im Besitz des Kunden	Schreiben	coip-pool*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateCoipPoolPermission [nur Berechtigung]	Erteilt die Berechtigung, einem Dienst den Zugriff auf einen IP-Pool (CoIP) im Besitz des Kunden zu erlauben	Schreiben	coip-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateCustomerGateway	Erteilt die Genehmigung zur Erstellung eines Kunden-Gateways, das Informationen AWS über Ihr Kunden-Gateway-Gerät bereitstellt	Schreiben	customer-gateway*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDefaultSubnet	Gewährt die Berechtigung, ein Standardsubnetz in einer angegebenen Availability Zone in einer Standard-VPC zu erstellen	Write		ec2:Region	
CreateDefaultVpc	Gewährt die Berechtigung zum Erstellen einer Standard-VPC mit einem Standardsubnetz in jeder Availability Zone	Write		ec2:Region	
CreateDhcpOptions	Gewährt die Berechtigung zum Erstellen einer Gruppe von DHCP-Optionen für eine VPC	Write	dhcp-options*	aws:RequestTag/${TagKey} aws:TagKeys ec2:DhcpOptionsID	ec2:CreateTags
				ec2:Region	
CreateEgressOnlyInternetGateway	Gewährt die Berechtigung, ein Internet-Gateway nur für ausgehenden Verkehr für eine VPC zu erstellen	Schreiben	egress-only-internet-gateway*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateFleet	Gewährt die Berechtigung zum Starten einer EC2-Flotte. Berechtigungen auf Ressourcenebene für diese Aktion beinhalten nicht die in einer Startvorlage festgelegten Ressourcen. Um Berechtigungen auf Ressourcenebene für Ressourcen anzugeben, die in einer Startvorlage angegeben sind, müssen Sie die Ressourcen in die RunInstances Aktionserklärung aufnehmen	Schreiben	fleet*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			instance*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceID ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:RootDeviceType ec2:Tenancy	
			image	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
			launch-template	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			placement-group	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			volume	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:Encrypted ec2:KmsKeyId ec2:ParentSnapshot ec2:VolumeID ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:VolumeType	
				ec2:Region	
CreateFlowLogs	Gewährt die Berechtigung, ein oder mehrere Ablauf-Protokolle zum Erfassen des IP-Datenverkehrs für eine Netzwerkschnittstelle zu erstellen	Write	vpc-flow-log*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags iam:PassRole
			network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
			transit-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			vpc	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateFpgaImage	Gewährt die Berechtigung, ein Amazon FPGA-Image (AFI) aus einem Designcheckpoint (DCP) zu erstellen	Write	fpga-image*	aws:RequestTag/${TagKey} aws:TagKeys ec2:Owner ec2:Public	ec2:CreateTags
				ec2:Region	
CreateImage	Gewährt die Berechtigung, ein Amazon EBS-Backed AMI aus einer gestoppten oder ausgeführten Amazon EBS-gestützten Instance zu erstellen	Schreiben	image*	aws:RequestTag/${TagKey} aws:TagKeys ec2:ImageID ec2:Owner	ec2:CreateTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			snapshot*	aws:RequestTag/${TagKey} aws:TagKeys ec2:OutpostArn ec2:Owner ec2:ParentVolume ec2:SnapshotID ec2:SnapshotTime ec2:SourceOutpostArn ec2:VolumeSize	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateInstanceConnectEndpoint	Gewährt die Berechtigung, einen EC2-Instance-Connect-Endpunkt zu erstellen, mit dem Sie eine Verbindung zu einer Instance ohne öffentliche IPv4-Adresse herstellen können	Schreiben	instance-connect-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys ec2:SubnetID	ec2:CreateTags
			subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
				ec2:Region	
CreateInstanceEventWindow	Gewährt die Berechtigung zum Erstellen eines Ereignisfensters, in dem geplante Ereignisse für die zugeordneten Amazon EC2 Instances ausgeführt werden können	Schreiben	instance-event-window*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	
CreateInstanceExportTask	Gewährt die Berechtigung zum Exportieren einer ausgeführten oder gestoppten Instance in einen Amazon-S3-Bucket	Write	export-instance-task*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateInternetGateway	Gewährt die Berechtigung zum Erstellen eines Internet-Gateways für eine VPC	Schreiben	internet-gateway*	aws:RequestTag/${TagKey} aws:TagKeys ec2:InternetGatewayID	ec2:CreateTags
				ec2:Region	
CreateIpam	Gewährt die Berechtigung zum Erstellen eines Amazon VPC IP Address Manager (IPAM)	Schreiben	ipam*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags iam:CreateServiceLinkedRole
				ec2:Region	
CreateIpamPool	Gewährt die Berechtigung zum Erstellen eines IP-Adress pools für Amazon VPC IP Address Manager (IPAM), bei dem es sich um eine Sammlung zusammenhängender IP-Adress-CIDRs handelt	Schreiben	ipam-pool*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			ipam-scope*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateIpamResourceDiscovery	Gewährt die Berechtigung zum Erstellen einer IPAM-Ressourcenerfassung	Schreiben	ipam-resource-discovery*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags iam:CreateServiceLinkedRole
				ec2:Region	
CreateIpamScope	Gewährt die Berechtigung zum Erstellen eines Amazon VPC IP Address Manager (IPAM)-Bereichs, bei dem es sich um den Container auf höchster Ebene innerhalb von IPAM handelt	Schreiben	ipam*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			ipam-scope*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	
CreateKeyPair	Gewährt die Berechtigung zum Erstellen eines 2048-Bit-RSA-Schlüsselpaars	Write	key-pair*	aws:RequestTag/${TagKey} aws:TagKeys ec2:KeyPairType	ec2:CreateTags
				ec2:Region	
CreateLaunchTemplate	Gewährt die Berechtigung zum Erstellen einer Startvorlage	Write	launch-template*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags ssm:GetParameters
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateLaunchTemplateVersion	Gewährt die Berechtigung zum Erstellen einer neuen Version einer Startvorlage	Write	launch-template*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ssm:GetParameters
				ec2:Region	
CreateLocalGatewayRoute	Gewährt die Berechtigung zum Erstellen einer statischen Route die Routing-Tabelle eines lokalen Gateways	Schreiben	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			local-gateway-virtual-interface-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
			prefix-list	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateLocalGatewayRouteTable	Erteilt die Berechtigung zum Erstellen einer Routing-Tabelle eines lokalen Gateways	Schreiben	local-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			local-gateway-route-table*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	
CreateLocalGatewayRouteTablePermission [nur Berechtigung]	Erteilt die Berechtigung, einem Dienst den Zugriff auf eine Routing-Tabelle eines lokalen Gateways zu erlauben	Schreiben	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateLocalGatewayRouteTableVirtualInterfaceGroupAssociation	Erteilt die Berechtigung zum Erstellen einer Gruppenzugehörigkeit der virtuellen Schnittstellengruppe für die lokale Gateway-Routing-Tabelle	Schreiben	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			local-gateway-route-table-virtual-interface-group-association*	aws:RequestTag/${TagKey} aws:TagKeys	
			local-gateway-virtual-interface-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateLocalGatewayRouteTableVpcAssociation	Gewährt die Berechtigung, eine VPC mit einer Routing-Tabelle des lokalen Gateways zu verknüpfen	Write	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			local-gateway-route-table-vpc-association*	aws:RequestTag/${TagKey} aws:TagKeys	
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateManagedPrefixList	Gewährt die Berechtigung zum Erstellen einer verwalteten Präfixliste	Write	prefix-list*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	
CreateNatGateway	Gewährt die Berechtigung zum Erstellen eines NAT-Gateways in einem Subnetz	Write	natgateway*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			elastic-ip	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateNetworkAcl	Gewährt die Berechtigung zum Erstellen einer Netzwerk-ACL in einer VPC	Write	network-acl*	aws:RequestTag/${TagKey} aws:TagKeys ec2:NetworkAclID	ec2:CreateTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
CreateNetworkAclEntry	Gewährt die Berechtigung zum Erstellen eines nummerierten Eintrags (einer Regel) in einer Netzwerk-ACL	Schreiben	network-acl*	aws:ResourceTag/${TagKey} ec2:NetworkAclID ec2:ResourceTag/${TagKey} ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateNetworkInsightsAccessScope	Gewährt die Berechtigung zum Erstellen eines Netzwerkzugriff-Bereichs	Schreiben	network-insights-access-scope*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	
CreateNetworkInsightsPath	Gewährt die Berechtigung, einen Pfad zum Analysieren der Erreichbarkeit zu erstellen	Write	network-insights-path*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			instance	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			internet-gateway	aws:ResourceTag/${TagKey} ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	
			network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transit-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	
			vpc-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			vpc-endpoint-service	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			vpc-peering-connection	aws:ResourceTag/${TagKey} ec2:AccepterVpc ec2:RequesterVpc ec2:ResourceTag/${TagKey} ec2:VpcPeeringConnectionID	
			vpn-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateNetworkInterface	Gewährt die Berechtigung zum Erstellen einer Netzwerkschnittstelle in einem Subnetz	Schreiben	network-interface*	aws:RequestTag/${TagKey} aws:TagKeys ec2:NetworkInterfaceID	ec2:CreateTags
			subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateNetworkInterfacePermission	Erteilt einem AWS-autorisierten Benutzer die Erlaubnis, eine Berechtigung zu erstellen, um bestimmte Operationen an einer Netzwerkschnittstelle auszuführen	Berechtigungsverwaltung	network-interface*	aws:ResourceTag/${TagKey} ec2:AuthorizedService ec2:AuthorizedUser ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:Permission ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreatePlacementGroup	Gewährt die Berechtigung zum Erstellen einer Platzierungsgruppe	Schreiben	placement-group*	aws:RequestTag/${TagKey} aws:TagKeys ec2:PlacementGroupName ec2:PlacementGroupStrategy	ec2:CreateTags
				ec2:Region	
CreatePublicIpv4Pool	Gewährt die Berechtigung zum Erstellen eines öffentlichen IPv4-Adresspools für öffentliche IPv4-CIDRs, die Sie besitzen und nach Amazon zur Verwaltung mit Amazon VPC IP Address Manager (IPAM) bringen	Schreiben	ipv4pool-ec2*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateReplaceRootVolumeTask	Gewährt die Berechtigung zum Erstellen einer Ersatz-Root-Volume-Aufgabe	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	ec2:CreateTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			replace-root-volume-task*	aws:RequestTag/${TagKey} aws:TagKeys	
			volume*	aws:RequestTag/${TagKey} aws:TagKeys ec2:VolumeID	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			image	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			snapshot	aws:ResourceTag/${TagKey} ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	
CreateReservedInstancesListing	Gewährt die Berechtigung, ein Angebot für Standard Reserved Instances zu erstellen, die im Reserved-Instance-Marketplace verkauft werden sollen	Schreiben		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateRestoreImageTask	Erteilt die Berechtigung zum Starten einer Aufgabe, die ein AMI aus einem S3-Objekt wiederherstellt, das zuvor mit CreateStoreImageTask	Schreiben	image*	aws:RequestTag/${TagKey} aws:TagKeys ec2:ImageID ec2:Owner	ec2:CreateTags
				ec2:Region	
CreateRoute	Gewährt die Berechtigung zum Erstellen einer Route in einer VPC-Routing-Tabelle	Write	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateRouteTable	Gewährt die Berechtigung zum Erstellen einer Routing-Tabelle für eine VPC	Write	route-table*	aws:RequestTag/${TagKey} aws:TagKeys ec2:RouteTableID	ec2:CreateTags
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSecurityGroup	Gewährt die Berechtigung zum Erstellen einer Sicherheitsgruppe	Write	security-group*	aws:RequestTag/${TagKey} aws:TagKeys ec2:SecurityGroupID	ec2:CreateTags
			vpc	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSnapshot	Gewährt die Berechtigung, einen Snapshot eines EBS-Volumes zu erstellen und ihn in Amazon S3 zu speichern	Write	snapshot*	aws:RequestTag/${TagKey} aws:TagKeys ec2:OutpostArn ec2:ParentVolume ec2:SnapshotID ec2:SourceOutpostArn ec2:VolumeSize	ec2:CreateTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			volume*	aws:ResourceTag/${TagKey} ec2:Encrypted ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSnapshots	Gewährt die Berechtigung, absturzkonsistente Snapshots mehrerer EBS-Volumes zu erstellen und in Amazon S3 zu speichern	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceID ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	ec2:CreateTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			snapshot*	aws:RequestTag/${TagKey} aws:TagKeys ec2:OutpostArn ec2:ParentVolume ec2:SnapshotID ec2:SourceOutpostArn ec2:VolumeSize	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			volume*	aws:ResourceTag/${TagKey} ec2:Encrypted ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSpotDatafeedSubscription	Gewährt die Berechtigung zum Erstellen eines Datenfeeds für Spot-Instances zum Anzeigen von Spot-Instance-Nutzungsprotokollen	Write		ec2:Region	
CreateStoreImageTask	Gewährt die Berechtigung zum Speichern eines AMI als einzelnes Objekt in einem S3 Bucket	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSubnet	Gewährt die Berechtigung zum Erstellen eines Subnetzes in einer VPC	Schreiben	subnet*	aws:RequestTag/${TagKey} aws:TagKeys ec2:SubnetID	ec2:CreateTags
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
			ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSubnetCidrReservation	Gewährt die Berechtigung zum Erstellen einer Kapazitätsreservierung	Schreiben		ec2:Region	
CreateTags	Gewährt die Berechtigung zum Hinzufügen oder Überschreiben von einem oder mehreren Tags für Amazon EC2-Ressourcen	Markieren	capacity-reservation	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			capacity-reservation-fleet	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			carrier-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			client-vpn-endpoint	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			coip-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			customer-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			dedicated-host	aws:ResourceTag/${TagKey} ec2:AutoPlacement ec2:AvailabilityZone ec2:HostRecovery ec2:InstanceType ec2:Quantity ec2:ResourceTag/${TagKey}	
			dhcp-options	aws:ResourceTag/${TagKey} ec2:DhcpOptionsID ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			egress-only-internet-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			elastic-gpu	aws:ResourceTag/${TagKey} ec2:ElasticGpuType ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			elastic-ip	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	
			export-image-task	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			export-instance-task	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			fleet	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			fpga-image	aws:ResourceTag/${TagKey} ec2:Owner ec2:Public ec2:ResourceTag/${TagKey}	
			host-reservation	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			image	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
			import-image-task	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			import-snapshot-task	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			instance	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			instance-connect-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SubnetID	
			instance-event-window	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			internet-gateway	aws:ResourceTag/${TagKey} ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			ipam	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			ipam-resource-discovery	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			ipam-resource-discovery-association	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			ipam-scope	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			ipv4pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			ipv6pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			key-pair	aws:ResourceTag/${TagKey} ec2:KeyPairName ec2:KeyPairType ec2:ResourceTag/${TagKey}	
			launch-template	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			local-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			local-gateway-route-table	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			local-gateway-route-table-virtual-interface-group-association	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			local-gateway-route-table-vpc-association	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			local-gateway-virtual-interface	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			local-gateway-virtual-interface-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			natgateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			network-acl	aws:ResourceTag/${TagKey} ec2:NetworkAclID ec2:ResourceTag/${TagKey} ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			network-insights-access-scope	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			network-insights-access-scope-analysis	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			network-insights-analysis	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			network-insights-path	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			network-interface	aws:ResourceTag/${TagKey} ec2:AuthorizedUser ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:Permission ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			placement-group	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	
			prefix-list	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			replace-root-volume-task	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			reserved-instances	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:InstanceType ec2:ReservedInstancesOfferingType ec2:ResourceTag/${TagKey} ec2:Tenancy	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			route-table	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
			security-group-rule	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			snapshot	aws:ResourceTag/${TagKey} ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
			spot-fleet-request	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			spot-instances-request	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
			subnet-cidr-reservation	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			traffic-mirror-filter	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			traffic-mirror-session	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			traffic-mirror-target	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transit-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transit-gateway-connect-peer	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayConnectPeerId	
			transit-gateway-multicast-domain	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transit-gateway-policy-table	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayPolicyTableId	
			transit-gateway-route-table	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transit-gateway-route-table-announcement	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableAnnouncementId	
			verified-access-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			verified-access-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			verified-access-instance	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			verified-access-policy	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			verified-access-trust-provider	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			volume	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:Encrypted ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			vpc	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
			vpc-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			vpc-endpoint-connection	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			vpc-endpoint-service	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			vpc-endpoint-service-permission	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			vpc-flow-log	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			vpc-peering-connection	aws:ResourceTag/${TagKey} ec2:AccepterVpc ec2:RequesterVpc ec2:ResourceTag/${TagKey} ec2:VpcPeeringConnectionID	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			vpn-connection	aws:ResourceTag/${TagKey} ec2:AuthenticationType ec2:DPDTimeoutSeconds ec2:GatewayType ec2:IKEVersions ec2:InsideTunnelCidr ec2:InsideTunnelIpv6Cidr ec2:Phase1DHGroup ec2:Phase1EncryptionAlgorithms	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Phase1IntegrityAlgorithms ec2:Phase1LifetimeSeconds ec2:Phase2DHGroup ec2:Phase2EncryptionAlgorithms ec2:Phase2IntegrityAlgorithms ec2:Phase2LifetimeSeconds ec2:RekeyFuzzPercentage ec2:RekeyMarginTimeSeconds	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:ReplayWindowSizePackets ec2:ResourceTag/${TagKey} ec2:RoutingType	
			vpn-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:CreateAction ec2:Region	
CreateTrafficMirrorFilter	Gewährt die Berechtigung zum Erstellen eines Traffic Mirror-Filters	Write	traffic-mirror-filter*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTrafficMirrorFilterRule	Gewährt die Berechtigung zum Erstellen einer Traffic-Mirror-Filter-Regel	Write	traffic-mirror-filter*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			traffic-mirror-filter-rule*		
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTrafficMirrorSession	Gewährt die Berechtigung zum Erstellen einer Traffic Mirror-Sitzung	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	ec2:CreateTags
			traffic-mirror-filter*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			traffic-mirror-session*	aws:RequestTag/${TagKey} aws:TagKeys	
			traffic-mirror-target*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateTrafficMirrorTarget	Gewährt die Berechtigung zum Erstellen eines Traffic Mirror-Ziels	Write	traffic-mirror-target*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			network-interface	aws:ResourceTag/${TagKey} ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey}	
			vpc-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpceServiceName ec2:VpceServiceOwner	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTransitGateway	Gewährt die Berechtigung zum Erstellen eines Transit-Gateways	Write	transit-gateway*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayId	ec2:CreateTags
				ec2:Region	
CreateTransitGatewayConnect	Gewährt die Berechtigung zum Erstellen eines Connect-Anhangs aus einem angegebenen Transit-Gateway-Anhang	Write	transit-gateway-attachment*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayAttachmentId	ec2:CreateTags
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTransitGatewayConnectPeer	Gewährt die Berechtigung zum Erstellen eines Connect-Peers zwischen einem Transit-Gateway und einer Appliance	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	ec2:CreateTags
			transit-gateway-connect-peer*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayConnectPeerId	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTransitGatewayMulticastDomain	Gewährt die Berechtigung zum Erstellen einer Multicast-Domain für ein Transit-Gateway	Write	transit-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	ec2:CreateTags
			transit-gateway-multicast-domain*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTransitGatewayPeeringAttachment	Gewährt die Berechtigung, eine Transit-Gateway-Peering-Anlage zwischen einem Anforderer- und einem Annehmer-Transit-Gateway anzufordern	Schreiben	transit-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	ec2:CreateTags
			transit-gateway-attachment*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayAttachmentId	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTransitGatewayPolicyTable	Erteilung der Genehmigung zur Erstellung einer Transit-Gateway-Richtlinientabelle	Schreiben	transit-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	ec2:CreateTags
			transit-gateway-policy-table*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayPolicyTableId	
				ec2:Region	
CreateTransitGatewayPrefixListReference	Gewährt die Berechtigung zum Erstellen einer Transit-Gateway-Präfixlistenreferenz	Write	prefix-list*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTransitGatewayRoute	Gewährt die Berechtigung zum Erstellen einer statischen Route für eine Transit-Gateway-Routing-Tabelle	Write	transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTransitGatewayRouteTable	Gewährt die Berechtigung zum Erstellen einer Routing-Tabelle für ein Transit-Gateway	Schreiben	transit-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	ec2:CreateTags
			transit-gateway-route-table*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayRouteTableId	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTransitGatewayRouteTableAnnouncement	Erteilung der Erlaubnis zur Erstellung einer Ankündigung für eine Transit-Gateway-Routing-Tabelle	Schreiben	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	ec2:CreateTags
			transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transit-gateway-route-table-announcement*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayRouteTableAnnouncementId	
				ec2:Region	
CreateTransitGatewayVpcAttachment	Gewährt die Berechtigung zum Anfügen einer VPC an ein Transit-Gateway	Schreiben	subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	ec2:CreateTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transit-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	
			transit-gateway-attachment*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayAttachmentId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
CreateVerifiedAccessEndpoint	Gewährt die Berechtigung zum Erstellen eines Endpunkts mit verifiziertem Zugriff	Schreiben	verified-access-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			verified-access-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			network-interface	aws:ResourceTag/${TagKey} ec2:AuthorizedUser ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:Permission ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateVerifiedAccessGroup	Gewährt die Berechtigung zum Erstellen einer Gruppe mit verifiziertem Zugriff	Schreiben	verified-access-group*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateVerifiedAccessInstance	Gewährt die Berechtigung zum Erstellen einer Instance mit verifiziertem Zugriff	Schreiben	verified-access-instance*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	
CreateVerifiedAccessTrustProvider	Gewährt die Berechtigung zum Erstellen eines verifizierten Vertrauensanbieters	Schreiben	verified-access-trust-provider*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateVolume	Gewährt die Berechtigung zum Erstellen eines EBS-Volumes	Write	volume*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:Encrypted ec2:KmsKeyId ec2:ParentSnapshot ec2:VolumeID ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput	ec2:CreateTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:VolumeType	
				ec2:Region	
CreateVpc	Gewährt die Berechtigung zum Erstellen einer VPC mit einem angegebenen CIDR-Block	Schreiben	vpc*	aws:RequestTag/${TagKey} aws:TagKeys ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:VpcID	ec2:CreateTags
			ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			ipv6pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateVpcEndpoint	Erteilt die Berechtigung zum Erstellen eines VPC-Endpunkts für einen Dienst AWS	Schreiben	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpcID	ec2:CreateTags route53:AssociateVPCWithHostedZone

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			vpc-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys ec2:VpceServiceName ec2:VpceServiceOwner	
			route-table	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID	
			subnet	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SubnetID	
				ec2:Region	
CreateVpcEndpointConnectionNotification	Gewährt die Berechtigung zum Erstellen einer Verbindungsbenachrichtigung für einen VPC-Endpunkt oder einen VPC-Endpunktservice	Schreiben	vpc-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			vpc-endpoint-service	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateVpcEndpointServiceConfiguration	Erteilt die Berechtigung zum Erstellen einer VPC-Endpunktdienstkonfiguration, zu der Dienstnutzer (AWS Konten, IAM-Benutzer und IAM-Rollen) eine Verbindung herstellen können	Schreiben	vpc-endpoint-service*	aws:RequestTag/${TagKey} aws:TagKeys ec2:VpceServicePrivateDnsName	ec2:CreateTags
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateVpcPeeringConnection	Gewährt die Berechtigung zum Anfordern einer VPC-Peering-Verbindung zwischen zwei VPCs	Write	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	ec2:CreateTags
			vpc-peering-connection*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AccepterVpc ec2:RequesterVpc ec2:VpcPeeringConnectionID	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateVpnConnection	Gewährt die Berechtigung zum Erstellen einer VPN-Verbindung zwischen einem Virtual Private Gateway oder Transit-Gateway und einem Kunden-Gateway	Write	customer-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			vpn-connection*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AuthenticationType ec2:DPDTimeoutSeconds ec2:GatewayType ec2:IKEVersions ec2:InsideTunnelCidr ec2:InsideTunnelIpv6Cidr ec2:Phase1DHGroup ec2:Phase1Encrypti	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				onAlgorithms ec2:Phase1IntegrityAlgorithms ec2:Phase1LifetimeSeconds ec2:Phase2DHGroup ec2:Phase2EncryptionAlgorithms ec2:Phase2IntegrityAlgorithms ec2:Phase2LifetimeSeconds ec2:RekeyFuzzPercentage	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:RekeyMarginTimeSeconds ec2:ReplayWindowSizePackets ec2:RoutingType	
			transit-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			vpn-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateVpnConnectionRoute	Gewährt die Berechtigung zum Erstellen einer statischen Route für eine VPN-Verbindung zwischen einem Virtual Private Gateway und einem Kunden-Gateway	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateVpnGateway	Gewährt die Berechtigung zum Erstellen eines Virtual Private Gateways	Write	vpn-gateway*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	
DeleteCarrierGateway	Gewährt die Berechtigung zum Löschen eines Carrier-Gateways	Write	carrier-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteClientVpnEndpoint	Gewährt die Berechtigung zum Löschen eines Client-VPN-Endpunkts	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteClientVpnRoute	Gewährt die Berechtigung zum Löschen einer Route von einem Client-VPN-Endpunkt	Schreiben	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	
DeleteCoipCidr	Erteilt die Berechtigung zum Löschen eines Bereichs von IP-Adressen (CoIP) im Besitz des Kunden	Schreiben	coip-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteCoipPool	Erteilt die Berechtigung zum Löschen eines Pools von IP-Adressen (CoIP) im Besitz des Kunden	Schreiben	coip-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteCoipPoolPermission [nur Berechtigung]	Erteilt die Berechtigung, einem Dienst den Zugriff auf einen IP-Pool (CoIP) im Besitz des Kunden zu verweigern	Schreiben	coip-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteCustomerGateway	Gewährt die Berechtigung zum Löschen eines Kunden-Gateways	Write	customer-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteDhcpOptions	Gewährt die Berechtigung zum Löschen einer Gruppe von DHCP-Optionen	Write	dhcp-options*	aws:ResourceTag/${TagKey} ec2:DhcpOptionsID ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteEgressOnlyInternetGateway	Gewährt die Berechtigung zum Löschen eines Internet-Gateways nur für ausgehenden Verkehr	Write	egress-only-internet-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteFleets	Gewährt die Berechtigung zum Löschen einer oder mehrerer EC2-Flotten	Write	fleet*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
DeleteFlowLogs	Gewährt die Berechtigung zum Löschen eines oder mehrerer Ablauf-Protokolle	Write	vpc-flow-log*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteFpgaImage	Gewährt die Berechtigung zum Löschen eines Amazon FPGA-Images (AFI)	Schreiben	fpga-image*	aws:ResourceTag/${TagKey} ec2:Owner ec2:Public ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteInstanceConnectEndpoint	Gewährt die Berechtigung, einen EC2-Instance-Connect-Endpunkt zu löschen	Schreiben	instance-connect-endpoint*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SubnetID	
				ec2:Region	
DeleteInstanceEventWindow	Gewährt die Berechtigung zum Löschen des angegebenen Ereignisses	Schreiben	instance-event-window*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteInternetGateway	Gewährt die Berechtigung zum Löschen eines Internet-Gateways	Schreiben	internet-gateway*	aws:ResourceTag/${TagKey} ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteIpam	Gewährt die Berechtigung, einen Amazon VPC IP Address Manager (IPAM) zu löschen und alle dem IPAM zugeordneten überwachten Daten zu entfernen, einschließlich der historischen Daten für CIDRs	Schreiben	ipam*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteIpamPool	Gewährt die Berechtigung zum Löschen eines Amazon VPC IP Address Manager (IPAM)-Pools	Schreiben	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
DeleteIpamResourceDiscovery	Gewährt die Berechtigung zum Löschen einer IPAM-Ressourcenerfassung	Schreiben	ipam-resource-discovery*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteIpamScope	Gewährt die Berechtigung zum Löschen des Bereichs für einen Amazon VPC IP Address Manager (IPAM)	Schreiben	ipam-scope*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteKeyPair	Gewährt die Berechtigung zum Löschen eines Schlüsselpaars durch Entfernen des öffentlichen Schlüssels aus Amazon EC2	Write	key-pair	aws:ResourceTag/${TagKey} ec2:KeyPairName ec2:KeyPairType ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteLaunchTemplate	Gewährt die Berechtigung zum Löschen einer Startvorlage und der zugehörigen Versionen	Write	launch-template*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteLaunchTemplateVersions	Gewährt die Berechtigung zum Löschen einer oder mehrerer Versionen einer Startvorlage	Write	launch-template*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteLocalGatewayRoute	Gewährt die Berechtigung zum Löschen einer Route aus der Routing-Tabelle eines lokalen Gateways	Schreiben	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			prefix-list	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteLocalGatewayRouteTable	Gewährt die Berechtigung zum Löschen einer Routing-Tabelle eines lokalen Gateways	Schreiben	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteLocalGatewayRouteTablePermission [nur Berechtigung]	Gewährt die Berechtigung, einem Dienst den Zugriff auf eine Routing-Tabelle eines lokalen Gateways zu verweigern	Schreiben	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteLocalGatewayRouteTableVirtualInterfaceGroupAssociation	Erteilt die Berechtigung zum Löschen einer Gruppenzugehörigkeit der virtuellen Schnittstellengruppe für die lokale Gateway-Routing-Tabelle	Schreiben	local-gateway-route-table-virtual-interface-group-association*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
DeleteLocalGatewayRouteTableVpcAssociation	Gewährt die Berechtigung zum Löschen einer Mapping zwischen einer VPC und einer Routing-Tabelle des lokalen Gateways	Write	local-gateway-route-table-vpc-association*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteManagedPrefixList	Gewährt die Berechtigung zum Löschen einer verwalteten Präfixliste	Write	prefix-list*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteNatGateway	Gewährt die Berechtigung zum Löschen eines NAT-Gateways	Write	natgateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
DeleteNetworkAcl	Gewährt die Berechtigung zum Löschen einer Netzwerk-ACL	Write	network-acl*	aws:ResourceTag/${TagKey} ec2:NetworkAclID ec2:ResourceTag/${TagKey} ec2:Vpc	
				ec2:Region	
DeleteNetworkAclEntry	Gewährt die Berechtigung zum Löschen eines Eintrags (einer Regel) für eingehenden oder ausgehenden Datenverkehr aus einer Netzwerk-ACL	Schreiben	network-acl*	aws:ResourceTag/${TagKey} ec2:NetworkAclID ec2:ResourceTag/${TagKey} ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteNetworkInsightsAccessScope	Gewährt die Berechtigung zum Löschen eines Netzwerkzugriff-Bereichs	Schreiben	network-insights-access-scope*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteNetworkInsightsAccessScopeAnalysis	Gewährt die Berechtigung zum Löschen einer Netzwerkzugriff-Bereich-Analyse	Schreiben	network-insights-access-scope-analysis*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteNetworkInsightsAnalysis	Gewährt die Berechtigung zum Löschen einer Analyse von Netzwerkerkenntnissen	Write	network-insights-analysis*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteNetworkInsightsPath	Gewährt die Berechtigung zum Löschen eines Pfads zu Netzwerkerkenntnissen	Write	network-insights-path*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteNetworkInterface	Gewährt die Berechtigung zum Löschen einer getrennten Netzwerkschnittstelle	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteNetworkInterfacePermission	Gewährt die Berechtigung zum Löschen einer mit einer Netzwerkschnittstelle verknüpften Berechtigung	Berechtigungsverwaltung	network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeletePlacementGroup	Gewährt die Berechtigung zum Löschen einer Platzierungsgruppe	Schreiben	placement-group	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeletePublicIpv4Pool	Gewährt die Berechtigung zum Löschen eines öffentlichen IPv4-Adresspools für öffentliche IPv4-CIDRs, die Sie besitzen und nach zur Verwaltung mit Amazon VPC IP Address Manager (IPAM) gebracht haben	Schreiben	ipv4pool-ec2*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteQueuedReservedInstances	Gewährt die Berechtigung zum Löschen der Käufe in der Warteschlange für die angegebenen Reserved Instances	Schreiben		ec2:Region	
DeleteResourcePolicy [nur Berechtigung]	Gewährt die Berechtigung zum Entfernen einer IAM-Richtlinie, die die kontoüber greifende Freigabe von einer Ressource ermöglicht	Schreiben	ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			placement-group	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			verified-access-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteRoute	Gewährt die Berechtigung zum Löschen einer Route aus einer Routing-Tabelle	Write	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteRouteTable	Gewährt die Berechtigung zum Löschen einer Routing-Tabelle	Write	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
				ec2:Region	
DeleteSecurityGroup	Gewährt die Berechtigung zum Löschen einer Sicherheitsgruppe	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteSnapshot	Gewährt die Berechtigung zum Löschen eines Snapshots eines EBS-Volumes	Write	snapshot*	aws:ResourceTag/${TagKey} ec2:OutpostArn ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	
DeleteSpotDatafeedSubscription	Gewährt die Berechtigung zum Löschen eines Datenfeeds für Spot-Instances	Write		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteSubnet	Gewährt die Berechtigung zum Löschen eines Subnetzes	Schreiben	subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	
DeleteSubnetCidrReservation	Gewährt die Berechtigung zum Löschen einer abgelaufenen Reservierung.	Schreiben		ec2:Region	
DeleteTags	Gewährt die Berechtigung zum Löschen eines oder mehrerer Tags von Amazon EC2-Ressourcen	Markieren	capacity-reservation	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			capacity-reservation-fleet	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			carrier-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			client-vpn-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			coip-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			customer-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			dedicated-host	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			dhcp-options	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			egress-only-internet-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			elastic-gpu	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			elastic-ip	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			export-image-task	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			export-instance-task	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			fleet	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			fpga-image	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			host-reservation	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			image	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			import-image-task	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			import-snapshot-task	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			instance	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			instance-connect-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			instance-event-window	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			internet-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			ipam	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			ipam-resource-discovery	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			ipam-resource-discovery-association	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			ipam-scope	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			ipv4pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			ipv6pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			key-pair	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			launch-template	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			local-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			local-gateway-route-table	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			local-gateway-route-table-virtual-interface-group-association	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			local-gateway-route-table-vpc-association	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			local-gateway-virtual-interface	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			local-gateway-virtual-interface-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			natgateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			network-acl	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			network-insights-access-scope	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			network-insights-access-scope-analysis	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			network-insights-analysis	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			network-insights-path	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			network-interface	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			placement-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			prefix-list	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			replace-root-volume-task	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			reserved-instances	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			route-table	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			security-group-rule	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			snapshot	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			spot-fleet-request	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			spot-instances-request	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			subnet	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			subnet-cidr-reservation	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			traffic-mirror-filter	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			traffic-mirror-session	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			traffic-mirror-target	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			transit-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			transit-gateway-connect-peer	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			transit-gateway-multicast-domain	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			transit-gateway-policy-table	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transit-gateway-route-table	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			transit-gateway-route-table-announcement	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			verified-access-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			verified-access-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			verified-access-instance	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			verified-access-policy	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			verified-access-trust-provider	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			volume	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			vpc	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			vpc-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			vpc-endpoint-connection	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			vpc-endpoint-service	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			vpc-endpoint-service-permission	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			vpc-flow-log	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			vpc-peering-connection	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			vpn-connection	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			vpn-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				aws:TagKeys ec2:Region	
DeleteTrafficMirrorFilter	Gewährt die Berechtigung zum Löschen eines Traffic Mirror-Filters	Write	traffic-mirror-filter*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteTrafficMirrorFilterRule	Gewährt die Berechtigung zum Löschen einer Traffic Mirror-Filterregel	Write	traffic-mirror-filter*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			traffic-mirror-filter-rule*		
				ec2:Region	
DeleteTrafficMirrorSession	Gewährt die Berechtigung zum Löschen einer Traffic Mirror-Sitzung	Write	traffic-mirror-session*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteTrafficMirrorTarget	Gewährt die Berechtigung zum Löschen eines Traffic Mirror-Ziels	Write	traffic-mirror-target*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteTransitGateway	Gewährt die Berechtigung zum Löschen eines Transit-Gateways	Write	transit-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	
				ec2:Region	
DeleteTransitGatewayConnect	Gewährt die Berechtigung zum Löschen eines Transit-Gateway-Connect-Anhangs	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteTransitGatewayConnectPeer	Gewährt die Berechtigung zum Löschen eines Transit-Gateway-Connect-Peers	Schreiben	transit-gateway-connect-peer*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayConnectPeerId	
				ec2:Region	
DeleteTransitGatewayMulticastDomain	Gewährt Berechtigungen zum Löschen einer Transit-Gateway-Multicast-Domain	Schreiben	transit-gateway-multicast-domain*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteTransitGatewayPeeringAttachment	Gewährt die Berechtigung zum Löschen einer Peering-Anlage von einem Transit-Gateway	Schreiben	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	
DeleteTransitGatewayPolicyTable	Erteilung der Erlaubnis zum Löschen einer Transit-Gateway-Richtlinientabelle	Schreiben	transit-gateway-policy-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayPolicyTableId	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteTransitGatewayPrefixListReference	Gewährt die Berechtigung zum Löschen einer Transit-Gateway-Präfixlistenreferenz	Write	prefix-list*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteTransitGatewayRoute	Gewährt die Berechtigung zum Löschen einer Route aus einer Routing-Tabelle eines Transit-Gateways	Write	transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
				ec2:Region	
DeleteTransitGatewayRouteTable	Gewährt die Berechtigung zum Löschen einer Routing-Tabelle für Transit Gateway	Schreiben	transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteTransitGatewayRouteTableAnnouncement	Erteilung der Erlaubnis zum Löschen einer Transit-Gateway-Routing-Tabellenankündigung	Schreiben	transit-gateway-route-table-announcement*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableAnnouncementId	
				ec2:Region	
DeleteTransitGatewayVpcAttachment	Gewährt die Berechtigung zum Löschen einer VPC-Anlage von einem Transit-Gateway	Schreiben	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteVerifiedAccessEndpoint	Gewährt die Berechtigung zum Löschen eines Endpunkts mit verifiziertem Zugriff	Schreiben	verified-access-endpoint*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteVerifiedAccessGroup	Gewährt die Berechtigung zum Löschen einer Gruppe mit verifiziertem Zugriff	Schreiben	verified-access-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteVerifiedAccessInstance	Gewährt die Berechtigung zum Löschen einer Instance mit verifiziertem Zugriff	Schreiben	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteVerifiedAccessTrustProvider	Gewährt die Berechtigung zum Löschen eines verifizierten Vertrauensanbieters	Schreiben	verified-access-trust-provider*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteVolume	Gewährt die Berechtigung zum Löschen eines EBS-Volumes	Write	volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:Encrypted ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
DeleteVpc	Gewährt die Berechtigung zum Löschen einer VPC	Write	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
DeleteVpcEndpointConnectionNotifications	Gewährt die Berechtigung zum Löschen einer oder mehrerer VPC-Endpunkt-Verbindungsbenachrichtigungen	Write	vpc-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			vpc-endpoint-service	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
DeleteVpcEndpointServiceConfigurations	Gewährt die Berechtigung zum Löschen einer oder mehrerer VPC-Endpunkt-Service-Konfigurationen	Write	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteVpcEndpoints	Gewährt die Berechtigung zum Löschen eines oder mehrerer VPC-Endpunkte	Write	vpc-endpoint*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpceServiceName	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteVpcPeeringConnection	Gewährt die Berechtigung zum Löschen einer VPC-Peering-Verbindung	Write	vpc-peering-connection*	aws:ResourceTag/${TagKey} ec2:AccepterVpc ec2:RequesterVpc ec2:ResourceTag/${TagKey} ec2:VpcPeeringConnectionID	
				ec2:Region	
DeleteVpnConnection	Gewährt die Berechtigung zum Löschen einer VPN-Verbindung	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteVpnConnectionRoute	Gewährt die Berechtigung zum Löschen einer statischen Route für eine VPN-Verbindung zwischen einem Virtual Private Gateway und einem Kunden-Gateway	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteVpnGateway	Gewährt die Berechtigung zum Löschen eines Virtual Private Gateways	Write	vpn-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeprovisionByoipCidr	Gewährt die Berechtigung, einen IP-Adressbereich freizugeben, der durch Mitbringen eigener IP-Adressen (BYOIP) bereitgestellt wurde, und den entsprechenden Adresspool zu löschen	Schreiben		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeprovisionIpamByoasn	Gewährt die Berechtigung, die Bereitstellung einer Autonomen Systemnummer (ASN) von einem Amazon Web Services-Konto aufzuheben	Schreiben	ipam*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeprovisionIpamPoolCidr	Gewährt die Berechtigung, die Bereitstellung eines CIDR aus einem Amazon VPC IP Address Manager (IPAM)-Pool aufzuheben	Schreiben	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeprovisionPublicIpv4PoolCidr	Gewährt die Berechtigung, die Bereitstellung eines CIDR aus einem öffentlichen IPv4-Pool aufzuheben	Schreiben	ipv4pool-ec2*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeregisterImage	Gewährt die Berechtigung zum Aufheben der Registrierung eines Amazon Machine Image (AMI)	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	
DeregisterInstanceEventNotificationAttributes	Gewährt die Berechtigung zum Entfernen von Tags aus der Gruppe von Tags, die in Benachrichtigungen über geplante Ereignisse für Ihre Instances enthalten sind.	Write		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeregisterTransitGatewayMulticastGroupMembers	Gewährt die Berechtigung, die Registrierung eines oder mehrerer Netzwerkschnittstellenmitglieder bei einer Gruppen-IP-Adresse in einer Transit-Gateway-Multicast-Domain aufzuheben	Write	network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
			transit-gateway-multicast-domain	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
DeregisterTransitGatewayMulticastGroupSources	Gewährt die Berechtigung, die Registrierung einer oder mehrerer Netzwerkschnittstellenquellen bei einer Gruppen-IP-Adresse in einer Transit-Gateway-Multicast-Domain aufzuheben	Schreiben	network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transit-gateway-multicast-domain	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	
DescribeAccountAttributes	Erteilt die Berechtigung zur Beschreibung der Attribute von AWS-Konto	Auflisten		ec2:Region	
DescribeAddressTransfers	Gewährt die Berechtigung zum Beschreiben einer elastischen IP-Adressen-Übertragung	Auflisten		ec2:Region	
DescribeAddresses	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Elastic IP-Adressen	List		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeAddressesAttribute	Gewährt die Berechtigung zum Beschreiben der Attribute der angegebenen Elastic IP-Adressen	List	elastic-ip	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PubliclpAddress ec2:ResourceTag/${TagKey}	
				ec2:Region	
DescribeAggregateIdFormat	Gewährt die Berechtigung zum Beschreiben der Formateinstellungen für eine längere ID für alle Ressourcentypen	List		ec2:Region	
DescribeAvailabilityZones	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Availability Zones, die für Sie verfügbar sind	Auflisten		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeAwsNetworkPerformanceMetricSubscriptions	Gewährt die Berechtigung zum Beschreiben des aktuellen Abonnements für Infrastruktur-Leistungskennzahlen	Auflisten		ec2:Region	
DescribeBundleTasks	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Bündelungsaufgaben	List		ec2:Region	
DescribeByoipCidrs	Gewährt die Berechtigung zum Beschreiben der IP-Adressbereiche, die durch Mitbringen Ihrer eigenen IP-Adressen (BYOIP) bereitgestellt wurden	Auflisten		ec2:Region	
DescribeCapacityBlockOfferings	Gewährt die Berechtigung zum Beschreiben reservierter Kapazitätsangebote, die zum Kauf verfügbar sind	Auflisten		ec2:Region	
DescribeCapacityReservationFleets	Gewährt die Berechtigung zum Beschreiben einer oder mehrere Kapazitätsreservierungs-Flotten	Auflisten		ec2:Region	
DescribeCapacityReservations	Gewährt die Berechtigung zum Beschreiben einer oder mehrere Kapazitätsreservierungen	List		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeCarrierGateways	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer Carrier-Gateways	List		ec2:Region	
DescribeClassicLinkInstances	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer verknüpfter EC2-Classic-Instances	List		ec2:Region	
DescribeClientVpnAuthorizationRules	Gewährt die Berechtigung zum Beschreiben der Autorisierungsregeln für einen Client-VPN-Endpunkt	List	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeClientVpnConnections	Gewährt die Berechtigung zum Beschreiben von aktiven Clientverbindungen und Verbindungen, die innerhalb der letzten 60 Minuten für einen Client-VPN-Endpunkt beendet wurden	List	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeClientVpnEndpoints	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer Client-VPN-Endpunkte	List	client-vpn-endpoint	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeClientVpnRoutes	Gewährt die Berechtigung zum Beschreiben der Routen für einen Client-VPN-Endpunkt	List	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeClientVpnTargetNetworks	Gewährt die Berechtigung zum Beschreiben der Zielnetzwerke, die einem Client-VPN-Endpunkt zugeordnet sind	List	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeCoipPools	Gewährt die Berechtigung zum Beschreiben der angegebenen Adresspools des Kunden oder aller Adresspools des Kunden.	List		ec2:Region	
DescribeConversionTasks	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer Konvertierungsaufgaben	List		ec2:Region	
DescribeCustomerGateways	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer Kunden-Gateways	List		ec2:Region	
DescribeDhcpOptions	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer DHCP-Optionsgruppen	List		ec2:Region	
DescribeEgressOnlyInternetGateways	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer Internet-Gateways nur für ausgehenden Datenverkehr	List		ec2:Region	
DescribeElasticGpus	Gewährt die Berechtigung zum Beschreiben eines Elastic Graphics Accelerator, der einer Instance zugeordnet ist	Auflisten		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeExportImageTasks	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer Export-Image-Aufgaben	List		ec2:Region	
DescribeExportTasks	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Export-Instance-Aufgaben	Auflisten		ec2:Region	
DescribeFastLaunchImages	Gewährt die Berechtigung zum Beschreiben von schnellstartaktivierten Windows-AMIs	Auflisten		ec2:Region	
DescribeFastSnapshotRestores	Gewährt die Berechtigung zum Beschreiben des Status schneller Snapshot-Wiederherstellungen für Snapshots	Auflisten		ec2:Region	
DescribeFleetHistory	Gewährt die Berechtigung, die Ereignisse für eine EC2-Flotte während einer bestimmten Zeit zu beschreiben	List	fleet*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeFleetInstances	Gewährt die Berechtigung zum Beschreiben der ausgeführten Instances für eine EC2-Flotte	List	fleet*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DescribeFleets	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer EC2-Flotten	List		ec2:Region	
DescribeFlowLogs	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer Ablauf-Protokolle	List		ec2:Region	
DescribeFpgaImageAttribute	Gewährt die Berechtigung zum Beschreiben der Attribute eines Amazon FPGA-Images (AFI)	List	fpga-image*	aws:ResourceTag/${TagKey} ec2:Owner ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeFpgaImages	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer Amazon FPGA Images (AFIs)	List		ec2:Region	
DescribeHostReservationOfferings	Gewährt die Berechtigung, die Dedicated Host-Reservierungen zu beschreiben, die zum Kauf verfügbar sind	Auflisten		ec2:Region	
DescribeHostReservations	Erteilt die Berechtigung zur Beschreibung der Dedicated Host-Reservierungen, die Dedicated Hosts zugeordnet sind, in der AWS-Konto	Auflisten		ec2:Region	
DescribeHosts	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer Dedicated Hosts	List		ec2:Region	
DescribeIamInstanceProfileAssociations	Gewährt die Berechtigung zum Beschreiben der IAM-Instance-Profilmappingen	List		ec2:Region	
DescribeIdFormat	Gewährt die Berechtigung zum Beschreiben der ID-Formateinstellungen für Ressourcen	List		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeIdentityIdFormat	Gewährt die Berechtigung zum Beschreiben der ID-Formateinstellungen für Ressourcen für einen IAM-Benutzer, eine IAM-Rolle oder einen Root-Benutzer	List		ec2:Region	
DescribeImageAttribute	Gewährt die Berechtigung zum Beschreiben eines Attributs eines Amazon Machine Image (AMI)	List	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeImages	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer Images (AMIs, AKIs und ARIs)	List		ec2:Region	
DescribeImportImageTasks	Gewährt die Berechtigung, Aufgaben zum Importieren von virtuellen Maschinen oder zum Importieren von Snapshot-Aufgaben zu beschreiben	List		ec2:Region	
DescribeImportSnapshotTasks	Gewährt die Berechtigung, Aufgaben zum Importieren von Snapshots zu beschreiben	List		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeInstanceAttribute	Gewährt die Berechtigung zum Beschreiben der Attribute einer Instance	Auflisten	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeInstanceConnectEndpoints	Gewährt die Berechtigung, einen EC2-Instance-Connect-Endpunkt zu beschreiben	Auflisten		ec2:Region	
DescribeInstanceCreditSpecifications	Gewährt die Berechtigung zur Beschreibung der Kreditoption für die CPU-Auslastung einer oder mehrerer Burstable Performance-Instances	List		ec2:Region	
DescribeInstanceEventNotificationAttributes	Gewährt die Berechtigung zum Beschreiben der Tags, die in Benachrichtigungen über geplante Ereignisse für Ihre Instances enthalten sind.	Auflisten		ec2:Region	
DescribeInstanceEventWindows	Gewährt die Berechtigung zum Beschreiben der angegebenen Ereignisfenster oder aller Ereignisfenster	Auflisten		ec2:Region	
DescribeInstanceStatus	Gewährt die Berechtigung zum Beschreiben des Status einer oder mehrerer Instances	Auflisten		ec2:Region	
DescribeInstanceTopology	Gewährt die Berechtigung, eine baumbasierte Hierarchie zu beschreiben, die die physische Host-Platzierung von EC2-Instances darstellt	Auflisten		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeInstanceTypeOfferings	Gewährt die Berechtigung zum Beschreiben der Instance-Typen, die an einem Speicherort angeboten werden.	List		ec2:Region	
DescribeInstanceTypes	Gewährt die Berechtigung zum Beschreiben der Details von Instance-Typen, die an einem Speicherort angeboten werden.	List		ec2:Region	
DescribeInstances	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Instances	List		ec2:Region	
DescribeInternetGateways	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Internet-Gateways	Auflisten		ec2:Region	
DescribeIpamByoasn	Gewährt die Berechtigung, eine BYOASN (Bring Your Own Autonomous System Number) zu beschreiben, die Sie mit zu IPAM gebracht haben	Auflisten		ec2:Region	
DescribeIpamPools	Gewährt die Berechtigung zur Beschreibung von Amazon VPC IP Address Manager (IPAM)-Pools	Auflisten		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeIpamResourceDiscoveries	Gewährt die Berechtigung zum Beschreiben von IPAM-Ressourcenerfassungen	Auflisten		ec2:Region	
DescribeIpamResourceDiscoveryAssociations	Erteilt die Erlaubnis, Verknüpfungen zur Ressourcenerfassung mit einem Amazon VPC IPAM zu beschreiben	Auflisten		ec2:Region	
DescribeIpamScopes	Gewährt die Berechtigung zur Beschreibung von Amazon VPC IP Address Manager (IPAM)-Bereichen	Auflisten		ec2:Region	
DescribeIpams	Gewährt die Berechtigung zur Beschreibung eines Amazon VPC IP Address Manager (IPAM)	Auflisten		ec2:Region	
DescribeIpv6Pools	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer IPv6-Adresspools	List		ec2:Region	
DescribeKeyPairs	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer Schlüsselpaare	List		ec2:Region	
DescribeLaunchTemplateVersions	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Startvorlagen-Versionen	List		ec2:Region	ssm:GetParameters

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeLaunchTemplates	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Startvorlagen	Auflisten		ec2:Region	
DescribeLocalGatewayRouteTablePermissions [nur Berechtigung]	Erteilt die Berechtigung, einem Dienst die Beschreibung Routing-Tabellen-Berechtigungen des lokalen Gateways zu erlauben	Auflisten		ec2:Region	
DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations	Gewährt die Berechtigung zum Beschreiben der Mappings zwischen virtuellen Schnittstellengruppen und lokalen Gateway-Routing-Tabellen	List		ec2:Region	
DescribeLocalGatewayRouteTableVpcAssociations	Gewährt die Berechtigung zum Beschreiben einer Mapping zwischen VPCs und Routing-Tabellen des lokalen Gateways	List		ec2:Region	
DescribeLocalGatewayRouteTables	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Routing-Tabellen des lokalen Gateways	List		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeLocalGatewayVirtualInterfaceGroups	Gewährt die Berechtigung zum Beschreiben virtueller Schnittstellengruppen des lokalen Gateways	List		ec2:Region	
DescribeLocalGatewayVirtualInterfaces	Gewährt die Berechtigung zum Beschreiben virtueller Schnittstellen des lokalen Gateways	List		ec2:Region	
DescribeLocalGateways	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer lokaler Gateways	Auflisten		ec2:Region	
DescribeLockedSnapshots	Gewährt die Berechtigung zum Beschreiben des Sperrstatus für einen Snapshot	Auflisten		ec2:Region	
DescribeMacHosts	Erteilt die Erlaubnis zur Beschreibung Ihrer EC2 Mac-Dedicated Hosts	Auflisten		ec2:Region	
DescribeManagedPrefixLists	Erteilt die Erlaubnis, Ihre verwalteten Präfixlisten und alle AWS verwalteten Präfixlisten zu beschreiben	Auflisten		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeMovingAddresses	Gewährt die Berechtigung zum Beschreiben von Elastic IP-Adressen, die auf die EC2-VPC-Plattform verschoben werden	List		ec2:Region	
DescribeNatGateways	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer NAT-Gateways	List		ec2:Region	
DescribeNetworkAcls	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Netzwerk-ACLs	Auflisten		ec2:Region	
DescribeNetworkInsightsAccessScopeAnalyses	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Netzwerkzugriff-Bereich-Analysen	Auflisten		ec2:Region	
DescribeNetworkInsightsAccessScopes	Gewährt die Berechtigung zum Beschreiben der Netzwerkzugriff-Bereiche	Auflisten		ec2:Region	
DescribeNetworkInsightsAnalyses	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Netzwerkerkenntnis-Analysen	List		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeNetworkInsightsPaths	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer Netzwerkerkenntnis-Pfade	List		ec2:Region	
DescribeNetworkInterfaceAttribute	Gewährt die Berechtigung zum Beschreiben eines Netzwerkschnittstellenattributs	List		ec2:Region	
DescribeNetworkInterfacePermissions	Gewährt die Berechtigung zum Beschreiben der Berechtigungen, die einer Netzwerkschnittstelle zugeordnet sind	List		ec2:Region	
DescribeNetworkInterfaces	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Netzwerkschnittstellen	List		ec2:Region	
DescribePlacementGroups	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Platzierungsgruppen	Auflisten		ec2:Region	
DescribePrefixLists	Erteilt die Berechtigung, verfügbare AWS Dienste in einem Präfixlistenformat zu beschreiben	Auflisten		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribePrincipalIdFormat	Gewährt die Berechtigung zum Beschreiben der ID-Formateinstellungen für den Stammbenutzer und alle IAM-Rollen und IAM-Benutzer, die explizit eine längere ID-Einstellung (17-stellige ID) angegeben haben	List		ec2:Region	
DescribePublicIpv4Pools	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer IPv4-Adresspools	Auflisten		ec2:Region	
DescribeRegions	Erteilt die Erlaubnis, einen oder mehrere zu beschreiben AWS-Regionen , die derzeit in Ihrem Konto verfügbar sind	Auflisten		ec2:Region	
DescribeReplaceRootVolumeTasks	Gewährt die Berechtigung zum Beschreiben einer Ersatz-Root-Volume-Aufgabe	List		ec2:Region	
DescribeReservedInstances	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer erworbener Reserved Instances in Ihrem Konto	List		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeReservedInstancesListings	Gewährt die Berechtigung, die Reserved Instance-Angebote Ihres Kontos im Reserved Instance Marketplace zu beschreiben	List		ec2:Region	
DescribeReservedInstancesModifications	Gewährt die Berechtigung zum Beschreiben der an einer oder mehreren Reserved Instances vorgenommenen Änderungen	List		ec2:Region	
DescribeReservedInstancesOfferings	Gewährt die Berechtigung zum Beschreiben der Reserved Instance-Angebote, die zum Kauf verfügbar sind	List		ec2:Region	
DescribeRouteTables	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Routing-Tabellen	List		ec2:Region	
DescribeScheduledInstanceAvailability	Gewährt die Berechtigung zum Suchen verfügbarer Zeitpläne für geplante Instances	Auflisten		ec2:Region	
DescribeScheduledInstances	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer geplanter Instances in Ihrem Konto	Auflisten		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeSecurityGroupReferences	Gewährt die Berechtigung zum Beschreiben der VPCs auf der anderen Seite einer VPC-Peering-Verbindung, die auf bestimmte VPC-Sicherheitsgruppen verweisen	List		ec2:Region	
DescribeSecurityGroupRules	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Sicherheitsgruppen	List		ec2:Region	
DescribeSecurityGroups	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Sicherheitsgruppen	List		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeSnapshotAttribute	Gewährt die Berechtigung zum Beschreiben eines Attributs eines Snapshots	Auflisten	snapshot*	aws:ResourceTag/${TagKey} ec2:Encrypted ec2:OutpostArn ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:SourceOutpostArn ec2:VolumeSize	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeSnapshotTierStatus	Gewährt die Berechtigung zum Beschreiben des Speicherstufen-Status für Amazon-EBS-Snapshots	Auflisten		ec2:Region	
DescribeSnapshots	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer EBS-Snapshots	List		ec2:Region	
DescribeSpotDatafeedSubscription	Gewährt die Berechtigung zum Beschreiben des Datenfeeds für Spot-Instances	List		ec2:Region	
DescribeSpotFleetInstances	Gewährt die Berechtigung zum Beschreiben der ausgeführten Instances für eine Spot-Flotte	List	spot-fleet-request*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DescribeSpotFleetRequestHistory	Gewährt die Berechtigung, die Ereignisse für eine Spot-Flottenanforderung während einer bestimmten Zeit zu beschreiben	List	spot-fleet-request*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
DescribeSpotFleetRequests	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Spot-Flottenanforderungen	List		ec2:Region	
DescribeSpotInstanceRequests	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Spot-Instance-Anforderungen	List		ec2:Region	
DescribeSpotPriceHistory	Gewährt die Berechtigung zum Beschreiben des Spot-Instance-Preisverlaufs	List		ec2:Region	
DescribeStaleSecurityGroups	Gewährt die Berechtigung zum Beschreiben der veralteten Sicherheitsgruppenregeln für Sicherheitsgruppen in einer angegebenen VPC	List		ec2:Region	
DescribeStoreImageTasks	Gewährt die Berechtigung zum Beschreiben des Fortschritts der AMI-Speicheraufgaben	List		ec2:Region	
DescribeSubnets	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer Subnetze	List		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeTags	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer Tags für eine Amazon EC2-Ressource	Auflisten		ec2:Region	
DescribeTrafficMirrorFilters	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer Traffic Mirror-Filter	List		ec2:Region	
DescribeTrafficMirrorSessions	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Traffic-Spiegel-Sitzungen	List		ec2:Region	
DescribeTrafficMirrorTargets	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer Traffic Mirror-Ziele	List		ec2:Region	
DescribeTransitGatewayAttachments	Gewährt die Berechtigung, eine oder mehrere Anlagen zwischen Ressourcen und Transit-Gateways zu beschreiben	List		ec2:Region	
DescribeTransitGatewayConnectPeers	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer Transit-Gateway-Connect-Peers	List		ec2:Region	
DescribeTransitGatewayConnects	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer Transit-Gateway-Connect-Anhänge	List		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeTransitGatewayMulticastDomains	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Transit-Gateway-Multicastdomains	List		ec2:Region	
DescribeTransitGatewayPeeringAttachments	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Transit-Gateway-Peering-Anlagen	Auflisten		ec2:Region	
DescribeTransitGatewayPolicyTables	Erteilung der Erlaubnis zur Beschreibung einer Transit-Gateway-Richtlinientabelle	Auflisten		ec2:Region	
DescribeTransitGatewayRouteTableAnnouncements	Erteilung der Erlaubnis, eine Transit-Gateway-Routing-Tabelle-Ankündigung zu beschreiben	Auflisten		ec2:Region	
DescribeTransitGatewayRouteTables	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Routing-Tabellen des Transit-Gateways	List		ec2:Region	
DescribeTransitGatewayVpcAttachments	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer VPC-Anlagen auf einem Transit Gateway	List		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeTransitGateways	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer Transit-Gateways	Auflisten		ec2:Region	
DescribeTrunkInterfaceAssociations	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Netzwerkschnittstellen	Auflisten		ec2:Region	
DescribeVerifiedAccessEndpoints	Gewährt die Berechtigung zum Beschreiben der angegebenen Endpunkte mit verifiziertem Zugriff oder aller Endpunkte mit verifiziertem Zugriff	Auflisten		ec2:Region	
DescribeVerifiedAccessGroups	Gewährt die Berechtigung zum Beschreiben der angegebenen Gruppen mit verifiziertem Zugriff oder aller Gruppen mit verifiziertem Zugriff	Auflisten		ec2:Region	
DescribeVerifiedAccessInstanceLoggingConfigurations	Gewährt die Berechtigung zum Beschreiben der aktuellen Protokollierungskonfiguration für die Instances mit verifiziertem Zugriff	Auflisten		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeVerifiedAccessInstanceWebAclAssociations [nur Berechtigung]	Erteilt die Berechtigung, die Zuordnungen der AWS Web Application Firewall (WAF) der Web Access Control List (ACL) für eine Verified Access-Instanz zu beschreiben	Auflisten		ec2:Region	
DescribeVerifiedAccessInstances	Gewährt die Berechtigung zum Beschreiben der angegebenen Instances mit verifiziertem Zugriff oder aller Instances mit verifiziertem Zugriff	Auflisten		ec2:Region	
DescribeVerifiedAccessTrustProviders	Gewährt die Berechtigung zum Beschreiben von Details vorhandener Anbieter mit verifiziertem Zugriff	Auflisten		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeVolumeAttribute	Gewährt die Berechtigung zum Beschreiben eines Attributs eines EBS-Volumes	List	volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:Encrypted ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
DescribeVolumeStatus	Gewährt die Berechtigung zum Beschreiben des Status eines oder mehrerer EBS-Volumes	List		ec2:Region	
DescribeVolumes	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer EBS-Volumes	List		ec2:Region	
DescribeVolumesModifications	Gewährt die Berechtigung zum Beschreiben des aktuellen Änderungsstatus eines oder mehrerer EBS-Volumes	Auflisten		ec2:Region	
DescribeVpcAttribute	Gewährt die Berechtigung zum Beschreiben eines Attributs einer VPC	Auflisten	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeVpcClassicLink	Erteilt die Berechtigung, den ClassicLink Status einer oder mehrerer VPCs zu beschreiben	Auflisten		ec2:Region	
DescribeVpcClassicLinkDnsSupport	Erteilt die Erlaubnis, den ClassicLink DNS-Unterstützungsstatus einer oder mehrerer VPCs zu beschreiben	Auflisten		ec2:Region	
DescribeVpcEndpointConnectionNotifications	Gewährt die Berechtigung zum Beschreiben der Verbindungsbenachrichtigungen für VPC-Endpunkte und VPC-Endpunkt-Services	List		ec2:Region	
DescribeVpcEndpointConnections	Gewährt die Berechtigung zum Beschreiben der VPC-Endpunktverbindungen mit Ihren VPC-Endpunkt-Services	List		ec2:Region	
DescribeVpcEndpointServiceConfigurations	Gewährt die Berechtigung zum Beschreiben von VPC-Endpunkt-Service-Konfigurationen (Ihre Services)	List		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeVpcEndpointServicePermissions	Gewährt die Berechtigung zum Beschreiben der Prinzipale (Servicekonsumenten), denen es erlaubt ist, Ihren VPC-Endpunktservice zu erkennen	Auflisten	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DescribeVpcEndpointServices	Erteilt die Erlaubnis, alle unterstützten AWS Dienste zu beschreiben, die bei der Erstellung eines VPC-Endpunkts angegeben werden können	Auflisten		ec2:Region	
DescribeVpcEndpoints	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer VPC-Endpunkte	List		ec2:Region	
DescribeVpcPeeringConnections	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer VPC-Peering-Verbindungen	List		ec2:Region	
DescribeVpcs	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer VPCs	List		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeVpnConnections	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer VPN-Verbindungen	Auflisten		ec2:Region	
DescribeVpnGateways	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer Virtual Private Gateways	List		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DetachClassicLinkVpc	Gewährt die Berechtigung zum Aufheben der Verknüpfung (Trennen) einer verknüpften EC2-Classic-Instance von einer VPC	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceID ec2:InstanceMarketType ec2:InstanceProfile ec2:InstanceType ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DetachInternetGateway	Gewährt die Berechtigung zum Trennen eines Internet-Gateways von einer VPC	Write	internet-gateway*	aws:ResourceTag/${TagKey} ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DetachNetworkInterface	Gewährt die Berechtigung zum Trennen einer Netzwerkschnittstelle von einer Instance	Schreiben	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	
DetachVerifiedAccessTrustProvider	Gewährt die Berechtigung zum Trennen eines Vertrauensanbieters von einer Instance mit verifiziertem Zugriff	Schreiben	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			verified-access-trust-provider*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DetachVolume	Gewährt die Berechtigung zum Trennen eines EBS-Volumes von einer Instance	Write	volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:Encrypted ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			instance	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DetachVpnGateway	Gewährt die Berechtigung zum Trennen eines Virtual Private Gateway von einer VPC	Schreiben	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
			vpn-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisableAddressTransfer	Gewährt die Berechtigung zum Deaktivieren einer Übertragung einer Elastic-IP-Adresse	Schreiben	elastic-ip*	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	
				ec2:Region	
DisableAwsNetworkPerformanceMetricSubscription	Gewährt die Berechtigung zum Deaktivieren von Abonnements für Infrastruktur-Leistungskennzahlen	Schreiben		ec2:Region	
DisableEbsEncryptionByDefault	Gewährt die Berechtigung, die EBS-Verschlüsselung standardmäßig für Ihr Konto zu deaktivieren	Schreiben		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisableFastLaunch	Gewährt die Berechtigung zum Deaktivieren des Schnellstarts für Windows AMIs	Schreiben	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisableFastSnapshotRestores	Gewährt die Berechtigung zum Deaktivieren von schnellen Snapshot-Wiederherstellungen für einen oder mehrere Snapshots in angegebenen Availability Zones	Schreiben	snapshot*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisableImage	Gewährt die Berechtigung zum Deaktivieren eines AMI	Schreiben	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	
DisableImageBlockPublicAccess	Erteilt die Berechtigung, den öffentlichen Zugriff für AMIs auf der angegebenen Kontoebene zu deaktivieren AWS-Region	Schreiben		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisableImageDeprecation	Gewährt die Berechtigung zum Abbrechen der Ablehnung des angegebenen AMI	Schreiben	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	
DisableIpamOrganizationAdminAccount	Erteilt die Erlaubnis, ein Mitgliedskonto einer AWS Organizations als Amazon VPC IP Address Manager (IPAM) -Administratorkonto zu deaktivieren	Schreiben		ec2:Region	organizations:DeregisterDelegatedAdministrator

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisableSerialConsoleAccess	Gewährt die Berechtigung, den Zugriff auf die serielle EC2-Konsole aller Instances für Ihr Konto zu deaktivieren	Schreiben		ec2:Region	
DisableSnapshotBlockPublicAccess	Gewährt die Berechtigung zum Deaktivieren der Einstellung „Öffentlichen Zugriff für Schnappschüsse blockieren“ für eine Region	Schreiben		ec2:Region	
DisableTransitGatewayRouteTablePropagation	Gewährt die Berechtigung, eine Ressourcen-Anlage an der Propagierung von Routen in der angegebenen Propagierungs-Routing-Tabelle zu hindern	Write	transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			transit-gateway-route-table-announcement	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableAnnouncementId	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisableVgwRoutePropagation	Gewährt die Berechtigung, ein Virtual Private Gateway an der Propagierung von Routen in einer angegebenen Routing-Tabelle einer VPC zu hindern	Schreiben	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
			vpn-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisableVpcClassicLink	Erteilt die Deaktivierungsberechtigung ClassicLink für eine VPC	Schreiben	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
DisableVpcClassicLinkDnsSupport	Erteilt die Erlaubnis, die ClassicLink DNS-Unterstützung für eine VPC zu deaktivieren	Schreiben	vpc	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateAddress	Gewährt die Berechtigung, eine Elastic IP-Adresse von einer Instance oder einer Netzwerkschnittstelle zu trennen	Write	elastic-ip	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateClientVpnTargetNetwork	Gewährt die Berechtigung, die Mapping eines Zielnetzwerks zu einem Client-VPN-Endpunkt aufzuheben	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateEnclaveCertificateIamRole	Gewährt die Berechtigung, die Mapping eines ACM-Zertifikats zu einer IAM-Rolle aufzuheben	Write	certificate*		
			role*		
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateIamInstanceProfile	Gewährt die Berechtigung, die Mapping eines IAM-Instance-Profils zu einer ausgeführten oder gestoppten Instance aufzuheben	Schreiben	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateInstanceEventWindow	Gewährt die Berechtigung, die Zuordnung eines oder mehrerer Ziele zu einem Ereignisfenster aufzuheben	Schreiben	instance-event-window*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DisassociateIpamByoasn	Gewährt die Berechtigung, die Zuordnung einer Autonomen Systemnummer (ASN) zu einer BYOIP-CIDR zu trennen	Schreiben		ec2:Region	
DisassociateIpamResourceDiscovery	Gewährt die Berechtigung, die Verknüpfung einer Ressourcenerfassung von einem Amazon VPC IPAM zu trennen	Schreiben	ipam-resource-discovery-association*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateNatGatewayAddress	Gewährt die Berechtigung zum Aufheben der Zuordnung von sekundären Elastic-IP-Adressen zu einem öffentlichen NAT-Gateway	Schreiben	elastic-ip*	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	
			natgateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			network-interface*	aws:ResourceTag/${TagKey} ec2:AuthorizedUser ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:Permission ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateRouteTable	Gewährt die Berechtigung, die Mapping eines Subnetzes zu einer Routing-Tabelle aufzuheben	Write	internet-gateway	aws:ResourceTag/${TagKey} ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	
			ipv4pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			ipv6pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			route-table	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			vpn-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DisassociateSubnetCidrBlock	Gewährt die Berechtigung, die Mapping eines CIDR-Blocks zu einem Subnetz aufzuheben	Write	subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateTransitGatewayMulticastDomain	Gewährt die Berechtigung, die Mapping einer oder mehrerer Subnetze zu einer Transit-Gateway-Multicast-Domain aufzuheben	Schreiben	subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
			transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transit-gateway-multicast-domain*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	
DisassociateTransitGatewayPolicyTable	Erteilung der Erlaubnis, eine Richtlinientabelle von einem Transit-Gateway abzukoppeln	Schreiben	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transit-gateway-policy-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayPolicyTableId	
				ec2:Region	
DisassociateTransitGatewayRouteTable	Gewährt die Berechtigung, die Mapping einer Ressource n-Anlage zu einer Routing-Tabelle für Transit-Gateways aufzuheben	Schreiben	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
				ec2:Region	
DisassociateTrunkInterface	Gewährt die Berechtigung, eine Zweignetzwerkschnittstelle mit einer Trunk-Netzwerkschnittstelle zu	Schreiben		ec2:Region	
DisassociateVerifiedAccessInstanceWebAcl [nur Berechtigung]	Erteilt die Berechtigung, die Zuordnung einer AWS Web Application Firewall (WAF) Web Access Control List (ACL) zu einer Verified Access-Instanz zu trennen	Schreiben	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateVpcCidrBlock	Gewährt die Berechtigung, die Verbindung eines CIDR-Blocks mit einer VPC zu trennen	Schreiben	vpc	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
EnableAddressTransfer	Gewährt die Berechtigung zum Aktivieren einer Übertragung einer Elastic-IP-Adresse	Schreiben	elastic-ip*	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PubliclpAddress ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
EnableAwsNetworkPerformanceMetricSubscription	Gewährt die Berechtigung zum Aktivieren von Infrastrukturleistungsabonnements	Schreiben		ec2:Region	
EnableEbsEncryptionByDefault	Gewährt die Berechtigung, die EBS-Verschlüsselung für Ihr Konto standardmäßig zu aktivieren	Schreiben		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
EnableFastLaunch	Gewährt die Berechtigung zum Aktivieren des Schnellstarts für Windows AMIs	Schreiben	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
			launch-template	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
EnableFastSnapshotRestores	Gewährt die Berechtigung, schnelle Snapshot-Wiederherstellungen für einen oder mehrere Snapshots in angegebenen Availability Zones zu aktivieren	Schreiben	snapshot*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
EnableImage	Gewährt die Berechtigung zum erneuten Aktivieren eines deaktivierten AMI	Schreiben	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	
EnableImageBlockPublicAccess	Erteilt die Berechtigung, den öffentlichen Zugriff für AMIs auf Kontoebene im angegebenen Bereich zu aktivieren AWS-Region	Schreiben		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
EnableImageDeprecation	Gewährt die Berechtigung, das angegebene AMI zum angegebenen Datum und zu der angegebenen Uhrzeit zu verwerfen.	Schreiben	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
EnableIpamOrganizationAdminAccount	Erteilt die Erlaubnis, ein Mitgliedskonto einer AWS Organizations als Amazon VPC IP Address Manager (IPAM) -Administratorkonto zu aktivieren	Schreiben		ec2:Region	iam:CreateServiceLinkedRole organizations:EnableAWSServiceAccess organizations:RegisterDelegatedAdministrator
EnableReachabilityAnalyzerOrganizationSharing	Gewährt die Berechtigung zum Aktivieren der gemeinsamen Nutzung des Erreichbarkeitsanalysators durch die Organisation	Schreiben		ec2:Region	iam:CreateServiceLinkedRole organizations:EnableAWSServiceAccess
EnableSerialConsoleAccess	Gewährt die Berechtigung, den Zugriff auf die serielle EC2-Konsole aller Instances für Ihr Konto zu ermöglichen	Schreiben		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
EnableSnapshotBlockPublicAccess	Gewährt die Berechtigung, die Einstellung „Öffentlichen Zugriff für Snapshots blockieren“ für eine Region zu aktivieren oder zu ändern	Schreiben		ec2:Region	
EnableTransitGatewayRouteTablePropagation	Gewährt die Berechtigung, einer Anlage die Verteilung von Routen an eine Propagierungs-Routing-Tabelle zu ermöglichen	Write	transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transit-gateway-route-table-announcement	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableAnnouncementId	
				ec2:Region	
EnableVgwRoutePropagation	Gewährt die Berechtigung, einem Virtual Private Gateway die Propagierung von Routen in einer VPC-Routing-Tabelle zu ermöglichen	Write	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			vpn-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
EnableVolumeIO	Gewährt die Berechtigung zum Aktivieren von I/O-Vorgängen für ein Volume, für das I/O-Vorgänge deaktiviert wurden	Schreiben	volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:Encrypted ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
EnableVpcClassicLink	Erteilt die Erlaubnis, eine VPC zu aktivieren für ClassicLink	Schreiben	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
EnableVpcClassicLinkDnsSupport	Erteilt die Erlaubnis, einer VPC die Unterstützung der DNS-Hostnamenauflösung zu ermöglichen für ClassicLink	Schreiben	vpc	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ExportClientVpnClientCertificateRevocationList	Gewährt die Berechtigung zum Download der Clientzertifikatsperrliste für einen Client-VPN-Endpunkt	Lesen	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ExportClientVpnClientConfiguration	Gewährt die Berechtigung zum Download des Inhalts der Client-VPN-Endpunkt-Konfigurationsdatei für einen Client-VPN-Endpunkt	Lesen	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ExportImage	Gewährt die Berechtigung, ein Amazon Machine Image (AMI) in eine VM-Datei zu exportieren	Write	export-image-task*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ExportTransitGatewayRoutes	Gewährt die Berechtigung zum Exportieren von Routen aus einer Transit Gateway-Routing-Tabelle in einen Amazon-S3-Bucket	Write		ec2:Region	
GetAssociatedEnclaveCertificateIamRoles	Gewährt die Berechtigung zum Abrufen der Liste von Rollen, die einem ACM-Zertifikat zugeordnet sind	Read	certificate*		
				ec2:Region	
GetAssociatedIpv6PoolCidrs	Gewährt die Berechtigung zum Abrufen von Informationen über die IPv6-CIDR-Block-Mappings für einen angegebenen IPv6-Adresspool	Lesen		ec2:Region	
GetAwsNetworkPerformanceData	Gewährt die Berechtigung zum Abrufen von Netzwerkleistungsdaten	Lesen		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetCapacityReservationUsage	Gewährt die Berechtigung zum Abrufen von Nutzungsinformationen über eine Kapazitätsreservierung	Read	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:CapacityReservationFleet ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetCoipPoolUsage	Gewährt die Berechtigung zum Beschreiben der Zuweisungen aus dem angegebenen Adresspool des Kunden.	Read	coip-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetConsoleOutput	Gewährt die Berechtigung zum Abrufen der Konsolenausgabe für eine Instance	Read	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetConsoleScreenshot	Gewährt die Berechtigung zum Abrufen eines Screenshots im JPG-Format einer ausgeführten Instance	Read	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:NewInstanceProfile ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
GetDefaultCreditSpecification	Gewährt die Berechtigung, die Standardgutschriftoption für die CPU-Auslastung einer Burstable Performance Instance-Familie abzurufen.	Read		ec2:Region	
GetEbsDefaultKmsKeyId	Gewährt die Berechtigung, die ID des Standard-Kundenmasterschlüssels (CMK) für die EBS-Verschlüsselung standardmäßig abzurufen	Read		ec2:Region	
GetEbsEncryptionByDefault	Gewährt die Berechtigung, zu beschreiben, ob die EBS-Verschlüsselung standardmäßig für Ihr Konto aktiviert ist	Lesen		ec2:Region	
GetFlowLogsIntegrationTemplate	Erteilt die Erlaubnis, eine CloudFormation Vorlage zu generieren, um die Integration von VPC-Flow-Protokollen mit Amazon Athena zu optimieren	Lesen	vpc-flow-log*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetGroupsForCapacityReservation	Gewährt die Berechtigung zum Auflisten der Resource Groups, denen eine Kapazitätsreservierung hinzugefügt wurde	List	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:CapacityReservationFleet ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetHostReservationPurchasePreview	Gewährt die Berechtigung zur Vorschau eines Reservierungskaufs mit Konfigurationen, die denen eines Dedicated Hosts entsprechen	Lesen		ec2:Region	
GetImageBlockPublicAccessState	Erteilt die Erlaubnis, den aktuellen Status der Sperrung des öffentlichen Zugriffs für AMIs auf der angegebenen Kontoebene abzurufen AWS-Region	Lesen		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetInstanceMetadataDefaults	Erteilt die Berechtigung zum Anzeigen der Standardeinstellungen für den Instance-Metadatendienst (IMDS), die für Ihr Konto in der angegebenen Region festgelegt wurden	Auflisten		ec2:Region	
GetInstanceTypesFromInstanceRequirements	Gewährt die Berechtigung zum Anzeigen einer Liste von Instance-Typen mit angegebenen Instance-Attributen	Auflisten		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetInstanceUefiData	Gewährt die Berechtigung zum Abrufen der binären Darstellung des UEFI-Variablenspeichers	Lesen	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:NewInstanceProfile ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
GetIpamAddressHistory	Gewährt die Berechtigung zum Abrufen historischer Informationen über ein CIDR innerhalb eines Amazon VPC IP Address Manager (IPAM)-Bereichs	Lesen	ipam-scope*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetIpamDiscoveredAccounts	Gewährt die Berechtigung zum Abrufen von erkannten IPAM-Konten	Lesen	ipam-resource-discovery*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetIpamDiscoveredPublicAddresses	Gewährt die Berechtigung zum Abrufen der öffentlichen IP-Adressen, die von IPAM erkannt wurden	Lesen	ipam-resource-discovery*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
GetIpamDiscoveredResourceCidrs	Gewährt die Berechtigung zum Abrufen der Ressourcen-CIDRs, die im Rahmen einer Ressourcenerfassung überwacht werden.	Lesen	ipam-resource-discovery*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetIpamPoolAllocations	Gewährt die Berechtigung zum Abrufen einer Liste aller CIDR-Zuweisungen in einem Amazon VPC IP Address Manager (IPAM)-Pool	Auflisten	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetIpamPoolCidrs	Gewährt die Berechtigung zum Abrufen der CIDRs, die an einen Amazon VPC IP Address Manager (IPAM)-Pool bereitgestellt sind	Lesen	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
GetIpamResourceCidrs	Gewährt die Berechtigung zum Abrufen von Informationen zu den Ressourcen in einem Amazon VPC IP Address Manager (IPAM)-Bereich	Lesen	ipam-scope*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetLaunchTemplateData	Gewährt die Berechtigung zum Anfordern der Konfigurationsdaten der angegebenen Instance für die Verwendung mit einer neuen Startvorlage oder einer Startvorlagenversion	Read	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetManagedPrefixListAssociations	Gewährt die Berechtigung zum Abrufen von Informationen zu den Ressourcen, die der angegebenen verwalteten Präfixliste zugeordnet sind.	Read	prefix-list*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetManagedPrefixListEntries	Gewährt die Berechtigung zum Abrufen von Informationen zu den Einträgen für eine angegebene verwaltete Präfixliste	Lesen	prefix-list*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetNetworkInsightsAccessScopeAnalysisFindings	Gewährt die Berechtigung zum Abrufen der Ergebnisse für eine oder mehrere Netzwerkzugriff-Bereich-Analysen	Lesen	network-insights-access-scope-analysis*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetNetworkInsightsAccessScopeContent	Gewährt die Berechtigung zum Abrufen des Inhalts für einen angegebenen Netzwerkzugriff-Bereich	Lesen	network-insights-access-scope*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetPasswordData	Gewährt die Berechtigung zum Abrufen des verschlüsselten Administratorpassworts für eine ausgeführte Windows-Instance	Read	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetReservedInstancesExchangeQuote	Gewährt die Berechtigung zur Rückgabe eines Angebots und zum Austausch von Informationen für den Austausch einer oder mehrerer Convertible Reserved Instances gegen eine neue Convertible Reserved Instance	Lesen		ec2:Region	
GetResourcePolicy [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben einer IAM-Richtlinie, die die kontoüber greifende Freigabe ermöglicht	Lesen	ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			placement-group	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			verified-access-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetSecurityGroupsForVpc	Gewährt die Berechtigung zum Abrufen einer Liste von Sicherheitsgruppen für eine bestimmte VPC	Lesen	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
GetSerialConsoleAccessStatus	Gewährt die Berechtigung zum Abrufen des Zugriffsstatus Ihres Kontos auf die serielle EC2-Konsole aller Instances	Lesen		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetSnapshotBlockPublicAccessState	Gewährt die Berechtigung zum Abrufen des aktuellen Status der Einstellung „Öffentlichen Zugriff für Schnappschüsse blockieren“ für eine Region	Lesen		ec2:Region	
GetSpotPlacementScores	Gewährt die Berechtigung zur Berechnung der Spot-Placement-Bewertung für eine Region oder Availability Zone anhand der angegebenen Zielkapazität und den Computing-Anforderungen	Lesen		ec2:Region	
GetSubnetCidrReservations	Gewährt die Berechtigung zum Abrufen von Informationen über die Hub-Ressource in Ihrem Konto	Lesen		ec2:Region	
GetTransitGatewayAttachmentPropagations	Gewährt die Berechtigung zum Auflisten der Routing-Tabellen, an die eine Ressourcenanlage Routen weiterleitet	List		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetTransitGatewayMulticastDomainAssociations	Gewährt die Berechtigung zum Abrufen von Informationen zu den Mappings für eine Transit-Gateway-Multicast-Domain	Auflisten	transit-gateway-multicast-domain*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	
GetTransitGatewayPolicyTableAssociations	Erteilung der Erlaubnis zum Abrufen von Informationen über Zuordnungen für eine Transit-Gateway-Richtlinientabelle	Auflisten	transit-gateway-policy-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayPolicyTableId	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetTransitGatewayPolicyTableEntries	Erteilung der Erlaubnis, Informationen über Assoziationen für einen Transit-Gateway-Tabelleneintrag zu erhalten	Auflisten	transit-gateway-policy-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayPolicyTableId	
				ec2:Region	
GetTransitGatewayPrefixListReferences	Gewährt die Berechtigung zum Abrufen von Informationen über Präfixlistenreferenzen für eine Transit-Gateway-Routing-Tabelle	List		ec2:Region	
GetTransitGatewayRouteTableAssociations	Gewährt die Berechtigung zum Abrufen von Informationen zu Mappings für eine Routing-Tabelle des Transit-Gateways	List		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetTransitGatewayRouteTablePropagations	Gewährt die Berechtigung zum Anfordern von Informationen über die Routing-Tabellen-Propagierungen für eine Transit-Gateway-Routing-Tabelle	Auflisten		ec2:Region	
GetVerifiedAccessEndpointPolicy	Gewährt die Berechtigung zum Anzeigen der mit dem Endpunkt verbundenen Richtlinie mit verifiziertem Zugriff	Auflisten	verified-access-endpoint*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetVerifiedAccessGroupPolicy	Gewährt die Berechtigung zum Anzeigen der Inhalte der mit der Gruppe verbundenen Richtlinie mit verifiziertem Zugriff	Auflisten	verified-access-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetVerifiedAccessInstanceWebAcl [nur Berechtigung]	Erteilt die Berechtigung, die AWS Web Access Control List (ACL) der Web Application Firewall (WAF) für eine Verified Access-Instanz anzuzeigen	Auflisten	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetVpnConnectionDeviceSampleConfiguration	Erteilt die Berechtigung zum Herunterladen einer AWS bereitgestellten Beispielkonfigurationsdatei zur Verwendung mit dem Kunden-Gateway-Gerät	Auflisten	vpn-connection*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			vpn-connection-device-type*		
				ec2:Region	
GetVpnConnectionDeviceTypes	Gewährt die Berechtigung, eine Liste der Kunden-Gateway-Geräte zu erhalten, für die Beispielkonfigurationsdateien bereitgestellt werden können	Auflisten		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetVpnTunnelReplacementStatus	Gewährt die Berechtigung, verfügbare Wartungsereignisse für Tunnel-Endpunkte einzusehen	Auflisten	vpn-connection*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ImportByoipCidrToIpam [nur Berechtigung]	Gewährt die Berechtigung, bestehende BYOIP-IPv4-CIDRs zu IPAM zu übertragen	Schreiben	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ImportClientVpnClientCertificateRevocationList	Gewährt die Berechtigung zum Upload einer Clientzertifikatsperrliste auf einen Client-VPN-Endpunkt	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ImportImage	Gewährt die Berechtigung zum Importieren von Single- oder Multi-Volume-Datenträger-Images oder EBS-Snapshots in ein Amazon Machine Image (AMI)	Write	image*	aws:RequestTag/${TagKey} aws:TagKeys ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:RootDeviceType	ec2:CreateTags
			import-image-task*	aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			snapshot	aws:ResourceTag/${TagKey} ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ImportInstance	Gewährt die Berechtigung zum Erstellen einer Aufgabe zum Importieren einer Instance unter Verwendung von Metadaten aus einem Datenträger-Image	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:InstanceID ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:Encrypted ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ImportKeyPair	Gewährt die Berechtigung zum Importieren eines öffentlichen Schlüssels aus einem RSA-Schlüsselpaar, das mit einem Drittanbieter-Tool erstellt wurde	Write	key-pair*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	
ImportSnapshot	Gewährt die Berechtigung zum Importieren eines Datenträgers in einen EBS-Snapshot	Write	import-snapshot-task*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			snapshot*	aws:RequestTag/${TagKey} aws:TagKeys ec2:Owner ec2:ParentVolume ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ImportVolume	Gewährt die Berechtigung zum Erstellen einer Aufgabe zum Importieren eines Volumes unter Verwendung von Metadaten aus einem Datenträger-Image	Schreiben	volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:Encrypted ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
InjectApiError [nur Berechtigung]	Gewährt die Berechtigung, vorübergehend Fehler für Ziel-API-Anfragen einzufügen	Schreiben		ec2:FisActionId ec2:FisTargetArns ec2:Region	
ListImagesInRecycleBin	Gewährt die Berechtigung zum Auflisten der Amazon Machine Images (AMIs), die sich derzeit im Papierkorb befinden	Auflisten		ec2:Region	
ListSnapshotsInRecycleBin	Gewährt die Berechtigung zum Auflisten der Amazon-EBS-Snapshots, die sich derzeit im Recycle Bin befinden	Auflisten		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
LockSnapshot	Gewährt die Berechtigung, einen Amazon EBS-Snapshot entweder im Governance- oder Compliance-Modus zu sperren, um ihn vor versehentlichem oder böswilligem Löschen zu schützen	Schreiben	snapshot*	aws:ResourceTag/${TagKey} ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotCoolOffPeriod ec2:SnapshotID ec2:SnapshotLockDuration ec2:SnapshotTime ec2:VolumeSize	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
ModifyAddressAttribute	Gewährt die Berechtigung zum Ändern eines Attributs der angegebenen Elastic IP-Adresse	Write	elastic-ip*	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Attribute ec2:Attribute/${AttributeName} ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyAvailabilityZoneGroup	Gewährt die Berechtigung zum Ändern des Aktivierungsstatus für die Gruppen „Lokale Zone“ und „Wavelength-Zone“ für Ihr Konto	Write		ec2:Region	
ModifyCapacityReservation	Gewährt die Berechtigung, die Kapazität einer Kapazitätsreservierung und die Bedingungen zu ändern, unter denen sie freigesetzt werden soll	Schreiben	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:CapacityReservationFleet ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyCapacityReservationFleet	Gewährt die Berechtigung zum Ändern einer Kapazitätsreservierungsflotte	Schreiben	capacity-reservation-fleet*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	ec2:ModifyCapacityReservation
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyClientVpnEndpoint	Gewährt die Berechtigung zum Ändern eines Client-VPN-Endpunkts	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:SamlProviderArn ec2:ServerCertificateArn	
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
			vpc	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
ModifyDefaultCreditSpecification	Gewährt die Berechtigung, die Standardgutschriftoption auf Kontoebene für die CPU-Auslastung von Burstable Performance-Instances zu ändern.	Write		ec2:Region	
ModifyEbsDefaultKmsKeyId	Gewährt die Berechtigung, den Standard-Kundenmasterschlüssel (CMK) für die EBS-Verschlüsselung standardmäßig für Ihr Konto zu ändern	Write		ec2:Region	
ModifyFleet	Gewährt die Berechtigung zum Ändern einer EC2-Flotte	Write	fleet*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			image	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
			launch-template	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyFpgaImageAttribute	Gewährt die Berechtigung zum Ändern eines Attributs eines Amazon FPGA-Images (AFI)	Write	fpga-image*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:Owner ec2:Public ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyHosts	Gewährt die Berechtigung zum Ändern eines Dedicated Hosts	Write	dedicated-host*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifyIdFormat	Gewährt die Berechtigung zum Ändern des ID-Formats für eine Ressource	Write		ec2:Region	
ModifyIdentityIdFormat	Gewährt die Berechtigung, das ID-Format einer Ressource für einen bestimmten Prinzipal in Ihrem Konto zu ändern	Write		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyImageAttribute	Gewährt die Berechtigung zum Ändern eines Attributs eines Amazon Machine Image (AMI)	Write	image*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyInstanceAttribute	Gewährt die Berechtigung zum Ändern eines Attributs einer Instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:InstanceProfile ec2:InstanceType ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Tenancy	
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			volume	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:Encrypted ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyInstanceCapacityReservationAttributes	Gewährt die Berechtigung zum Ändern der Kapazitätsreservierungseinstellungen für eine gestoppte Instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:InstanceProfile ec2:InstanceType ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Tenancy	
			capacity-reservation	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyInstanceCreditSpecification	Gewährt die Berechtigung zum Ändern der Kreditoption für die CPU-Auslastung einer Instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:InstanceProfile ec2:InstanceType ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Tenancy	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyInstanceEventStartTime	Gewährt die Berechtigung zum Ändern der Startzeit für ein geplantes EC2-Instance-Ereignis	Schreiben	instance*	aws:ResourceTag/${TagKey} ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:InstanceType ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyInstanceEventWindow	Gewährt die Berechtigung zum Ändern des angegebenen Endpunkts	Schreiben	instance-event-window*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyInstanceMaintenanceOptions	Erteilt die Berechtigung zum Ändern des Wiederherstellungsverhaltens für eine Instance	Schreiben	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:InstanceProfile ec2:InstanceType ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Tenancy	
				ec2:Region	
ModifyInstanceMetadataDefaults	Erteilt die Berechtigung, die Standardeinstellungen für den Instanz-Metadatendienst (IMDS) für Ihr Konto in der angegebenen Region zu ändern	Schreiben		ec2:Attribute/${AttributeName} ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyInstanceMetadataOptions	Gewährt die Berechtigung zum Ändern der Metadatenoptionen für eine Instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:InstanceProfile ec2:InstanceType ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Tenancy	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyInstancePlacement	Gewährt die Berechtigung zum Ändern der Platzierungsattribute für eine Instance	Schreiben	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:InstanceProfile ec2:InstanceType ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Tenancy	
			dedicated-host	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			placement-group	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyIpam	Gewährt die Berechtigung zum Ändern der Konfigurationen eines Amazon VPC IP Address Managers (IPAM)	Schreiben	ipam*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifyIpamPool	Gewährt die Berechtigung zum Ändern der Konfigurationen eines Amazon VPC IP Address Manager (IPAM)-Pools	Schreiben	ipam-pool*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
ModifyIpamResourceCidr	Gewährt die Berechtigung zum Ändern der Konfigurationen einer Amazon VPC IP Address Manager (IPAM)-Ressourcen-CIDR	Schreiben	ipam-scope*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifyIpamResourceDiscovery	Gewährt die Berechtigung zum Ändern einer Ressourcenerfassung	Schreiben	ipam-resource-discovery*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyIpamScope	Gewährt die Berechtigung zum Ändern der Konfigurationen eines Amazon VPC IP Address Manager (IPAM)-Bereichs	Schreiben	ipam-scope*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifyLaunchTemplate	Gewährt die Berechtigung zum Ändern einer Startvorlage	Schreiben	launch-template*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
ModifyLocalGatewayRoute	Gewährt die Berechtigung zum Ändern einer lokalen Gateway-Route	Schreiben	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			local-gateway-virtual-interface-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			network-interface	aws:ResourceTag/${TagKey} ec2:AuthorizedUser ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:Permission ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
			prefix-list	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
ModifyManagedPrefixList	Gewährt die Berechtigung zum Ändern einer verwalteten Präfixliste	Write	prefix-list*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyNetworkInterfaceAttribute	Gewährt die Berechtigung zum Ändern eines Attributs einer Netzwerkschnittstelle	Schreiben	network-interface*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			instance	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyPrivateDnsNameOptions	Gewährt die Berechtigung zum Ändern der Optionen für Instanz-Hostnamen für die angegebene Instance	Schreiben	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:InstanceProfile ec2:InstanceType ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:NewInstanceProfile ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyReservedInstances	Gewährt die Berechtigung zum Ändern von Attributen einer oder mehrerer Reserved Instances	Write	reserved-instances *	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:InstanceType ec2:ReservedInstancesOfferingType ec2:ResourceTag/${TagKey} ec2:Tenancy	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifySecurityGroupRules	Gewährt die Berechtigung zum Ändern der Regeln einer Sicherheitsgruppe	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
			security-group-rule*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			prefix-list	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifySnapshotAttribute	Gewährt die Berechtigung zum Hinzufügen oder Entfernen von Berechtigungseinstellungen für einen Snapshot	Berechtigungsverwaltung	snapshot*	aws:ResourceTag/${TagKey} ec2:Add/group ec2:Add/userId ec2:Attribute ec2:Attribute/${AttributeName} ec2:Owner ec2:ParentVolume ec2:Remove/group ec2:Remove/userId ec2:ResourceTag/${TagKey} ec2:SnapshotID	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifySnapshotTier	Gewährt die Berechtigung zum Archivieren von Amazon-EBS-Snapshots	Schreiben	snapshot*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
ModifySpotFleetRequest	Gewährt die Berechtigung zum Ändern einer Spot-Flottenanforderung	Write	spot-fleet-request*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
			launch-template	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifySubnetAttribute	Gewährt die Berechtigung zum Ändern eines Attributs eines Subnetzes	Write	subnet*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyTrafficMirrorFilterNetworkServices	Gewährt die Berechtigung zum Zulassen oder Einschränken von Spiegelungsnetzwerk-Services	Write	traffic-mirror-filter*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifyTrafficMirrorFilterRule	Gewährt die Berechtigung zum Ändern einer Datenspiegelungsregel	Write	traffic-mirror-filter*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			traffic-mirror-filter-rule*	ec2:Attribute ec2:Attribute/${AttributeName}	
				ec2:Region	
ModifyTrafficMirrorSession	Gewährt die Berechtigung zum Ändern einer Traffic Mirror-Sitzung	Write	traffic-mirror-session*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
			traffic-mirror-filter	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			traffic-mirror-target	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifyTransitGateway	Gewährt die Berechtigung zum Ändern eines Transit-Gateways	Write	transit-gateway*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transit-gateway-route-table	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
				ec2:Region	
ModifyTransitGatewayPrefixListReference	Gewährt die Berechtigung zum Ändern einer Transit-Gateway-Präfixlistenreferenz	Write	prefix-list*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
ModifyTransitGatewayVpcAttachment	Gewährt die Berechtigung zum Ändern einer VPC-Anlage auf einem Transit-Gateway	Schreiben	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	
ModifyVerifiedAccessEndpoint	Gewährt die Berechtigung zum Ändern der Konfiguration eines Endpunkts mit verifiziertem Zugriff	Schreiben	verified-access-endpoint*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
			verified-access-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyVerifiedAccessEndpointPolicy	Gewährt die Berechtigung zum Ändern der angegebenen Endpunktsrichtlinie mit verifiziertem Zugriff	Schreiben	verified-access-endpoint*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifyVerifiedAccessGroup	Gewährt die Berechtigung zum Ändern der angegebenen Konfiguration der Gruppe mit verifiziertem Zugriff	Schreiben	verified-access-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			verified-access-instance	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyVerifiedAccessGroupPolicy	Gewährt die Berechtigung zum Ändern der angegebenen Gruppenrichtlinie mit verifiziertem Zugriff	Schreiben	verified-access-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifyVerifiedAccessInstance	Gewährt die Berechtigung zum Ändern der angegebenen Konfiguration der Instance mit verifiziertem Zugriff	Schreiben	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifyVerifiedAccessInstanceLoggingConfiguration	Gewährt die Berechtigung zum Ändern der Protokollierungskonfiguration für die angegebene Instance mit verifiziertem Zugriff	Schreiben	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyVerifiedAccessTrustProvider	Gewährt die Berechtigung zum Ändern der Konfiguration des angegebenen Vertrauensanbieters mit verifiziertem Zugriff	Schreiben	verified-access-trust-provider*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyVolume	Gewährt die Berechtigung zum Ändern der Parameter eines EBS-Volumes	Write	volume*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:Encrypted ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops ec2:VolumeSize	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyVolumeAttribute	Gewährt die Berechtigung zum Ändern eines Attributs eines Volumes	Write	volume*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:Encrypted ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops ec2:VolumeSize	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	
ModifyVpcAttribute	Gewährt die Berechtigung zum Ändern eines Attributs einer VPC	Write	vpc*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyVpcEndpoint	Gewährt die Berechtigung zum Ändern eines Attributs eines VPC-Endpunkts	Write	vpc-endpoint*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
			route-table	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyVpcEndpointConnectionNotification	Gewährt die Berechtigung zum Ändern einer Verbindungsbenachrichtigung für einen VPC-Endpunkt oder einen VPC-Endpunkt-Service	Write	vpc-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			vpc-endpoint-service	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyVpcEndpointServiceConfiguration	Gewährt die Berechtigung zum Ändern der Attribute einer VPC-Endpunkt-Service-Konfiguration	Schreiben	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:VpceServicePrivateDnsName	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyVpcEndpointServicePayerResponsibility	Gewährt die Berechtigung zum Ändern des Zahlers, der für einen VPC-Endpunkt-Service verantwortlich ist	Schreiben	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifyVpcEndpointServicePermissions	Gewährt die Berechtigung zum Ändern der Berechtigungen für einen VPC-Endpunkt-Service	Berechtigungsverwaltung	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
ModifyVpcPeeringConnectionOptions	Gewährt die Berechtigung zum Ändern der VPC-Peering-Verbindungsoptionen auf einer Seite einer VPC-Peering-Verbindung	Write	vpc-peering-connection*	aws:ResourceTag/${TagKey} ec2:AccepterVpc ec2:Attribute ec2:Attribute/${AttributeName} ec2:RequesterVpc ec2:ResourceTag/${TagKey} ec2:VpcPeeringConnectionID	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyVpcTenancy	Gewährt die Berechtigung zum Ändern des Instance-Tenancy-Attributs einer VPC	Write	vpc*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyVpnConnection	Gewährt die Berechtigung zum Ändern des Zielgateways einer Site-to-Site-VPN-Verbindung	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AuthenticationType ec2:DPDTimeoutSeconds ec2:GatewayType ec2:IKEVersions ec2:InsideTunnelCidr ec2:InsideTunnelIpv6Cidr	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Phase1DHGroup ec2:Phase1EncryptionAlgorithms ec2:Phase1IntegrityAlgorithms ec2:Phase1LifetimeSeconds ec2:Phase2DHGroup ec2:Phase2EncryptionAlgorithms ec2:Phase2IntegrityAlgorithms ec2:Phase2LifetimeSeconds	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:RekeyFuzzPercentage ec2:RekeyMarginTimeSeconds ec2:ReplayWindowSizePackets ec2:ResourceTag/${TagKey} ec2:RoutingType	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyVpnConnectionOptions	Gewährt die Berechtigung zum Ändern der Verbindungsoptionen für Ihre Site-to-Site-VPN-Verbindung	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifyVpnTunnelCertificate	Gewährt die Berechtigung zum Ändern des Zertifikats für eine Site-to-Site-VPN-Verbindung	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyVpnTunnelOptions	Gewährt die Berechtigung zum Ändern der Optionen für eine Site-to-Site-VPN-Verbindung	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AuthenticationType ec2:DPDTimeoutSeconds ec2:GatewayType ec2:IKEVersions ec2:InsideTunnelCidr ec2:InsideTunnelIpv6Cidr	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Phase1DHGroup ec2:Phase1EncryptionAlgorithms ec2:Phase1IntegrityAlgorithms ec2:Phase1LifetimeSeconds ec2:Phase2DHGroup ec2:Phase2EncryptionAlgorithms ec2:Phase2IntegrityAlgorithms ec2:Phase2LifetimeSeconds	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:RekeyFuzzPercentage ec2:RekeyMarginTimeSeconds ec2:ReplayWindowSizePackets ec2:ResourceTag/${TagKey} ec2:RoutingType	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
MonitorInstances	Gewährt die Berechtigung, eine detaillierte Überwachung für eine derzeit ausgeführte Instance zu aktivieren.	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
MoveAddressToVpc	Gewährt die Berechtigung, eine Elastic IP-Adresse von der EC2-Classic-Plattform auf die EC2-VPC-Plattform zu verschieben	Schreiben		ec2:Region	
MoveByoipCidrToIpam	Gewährt die Berechtigung zum Verschieben eines BYOIP IPv4 CIDR aus einem öffentlichen IPv4-Pool in Amazon VPC IP Address Manager (IPAM)	Schreiben	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PauseVolumeIO [nur Berechtigung]	Gewährt die Berechtigung zum vorübergehenden Aussetzen von I/O-Vorgängen für ein Amazon EBS Ziel-Volume	Schreiben	volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:Encrypted ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			instance	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
ProvisionByoipCidr	Erteilt die Erlaubnis, einen Adressbereich für die Verwendung AWS mithilfe von Bring Your Own IP-Adressen (BYOIP) bereitzustellen und einen entsprechenden Adresspool zu erstellen	Schreiben		ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ProvisionIpamByoasn	Gewährt die Berechtigung zum Bereitstellen einer autonomen Systemnummer (ASN) zur Verwendung in einem Amazon Web Services-Konto	Schreiben	ipam*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ProvisionIpamPoolCidr	Gewährt die Berechtigung zum Bereitstellen eines CIDR an einen Amazon VPC IP Address Manager (IPAM)-Pool	Schreiben	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ProvisionPublicIpv4PoolCidr	Gewährt die Berechtigung zum Bereitstellen eines CIDR für einen öffentlichen IPv4-Pool	Schreiben	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			ipv4pool-ec2*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
PurchaseCapacityBlock	Gewährt die Berechtigung zum Kauf eines Angebots über reservierte Kapazitäten.	Schreiben	capacity-reservation*	aws:RequestTag/${TagKey} aws:TagKeys ec2:CapacityReservationFleet	ec2:CreateTags
				ec2:Region	
PurchaseHostReservation	Gewährt die Berechtigung zum Kauf einer Reservierung mit Konfigurationen, die denen eines Dedicated Hosts entsprechen	Write	dedicated-host*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
PurchaseReservedInstancesOffering	Gewährt die Berechtigung zum Kauf eines Reserved Instance-Angebots	Write		ec2:Region	
PurchaseScheduledInstances	Gewährt die Berechtigung zum Kauf einer oder mehrerer geplanter Instances mit einem bestimmten Zeitplan	Schreiben		ec2:Region	
PutResourcePolicy [nur Berechtigung]	Gewährt die Berechtigung zum Anfügen einer IAM-Richtlinie, die die kontoüber greifende Freigabe für eine Ressource ermöglicht	Schreiben	ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			placement-group	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	
			verified-access-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RebootInstances	Gewährt die Berechtigung, einen Neustart einer oder mehrerer Instances anzufordern	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RegisterImage	Gewährt die Berechtigung zum Registrieren einer Amazon Machine Image (AMI)	Write	image*	aws:RequestTag/${TagKey} aws:TagKeys ec2:ImageID ec2:Owner	ec2:CreateTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			snapshot	aws:ResourceTag/${TagKey} ec2:OutpostArn ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:SourceOutpostArn ec2:VolumeSize	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RegisterInstanceEventNotificationAttributes	Gewährt die Berechtigung zum Hinzufügen von Tags zum Satz von Tags, die in Benachrichtigungen über geplante Ereignisse für Ihre Instances enthalten sind	Write		ec2:Region	
RegisterTransitGatewayMulticastGroupMembers	Gewährt die Berechtigung, eine oder mehrere Netzwerkschnittstellen als Mitglied einer Gruppen-IP-Adresse in einer Transit-Gateway-Multicast-Domain zu registrieren	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transit-gateway-multicast-domain*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RegisterTransitGatewayMulticastGroupSources	Gewährt die Berechtigung, eine oder mehrere Netzwerkschnittstellen als Quelle einer Gruppen-IP-Adresse in einer Transit-Gateway-Multicast-Domain zu registrieren	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
			transit-gateway-multicast-domain*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
RejectTransitGatewayMulticastDomainAssociations	Gewährt die Berechtigung, Anforderungen zum Zuordnen von kontoübergreifenden Subnetzen zu einer Transit-Gateway-Multicast-Domain abzulehnen	Write	transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			transit-gateway-multicast-domain	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RejectTransitGatewayPeeringAttachment	Gewährt die Berechtigung zum Ablehnen einer Transit-Gateway-Peering-Anlagenanforderung	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	
RejectTransitGatewayVpcAttachment	Gewährt die Berechtigung, eine Anforderung zum Zuordnen einer VPC zu einem Transit-Gateway abzulehnen	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RejectVpcEndpointConnections	Gewährt die Berechtigung zum Ablehnen einer oder mehrerer VPC-Endpunktverbindungsanforderungen an einen VPC-Endpunkt-Service	Write	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
RejectVpcPeeringConnection	Gewährt die Berechtigung zum Ablehnen einer VPC-Peering-Verbindungsanforderung	Write	vpc-peering-connection*	aws:ResourceTag/${TagKey} ec2:AccepterVpc ec2:RequesterVpc ec2:ResourceTag/${TagKey} ec2:VpcPeeringConnectionID	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ReleaseAddress	Gewährt die Berechtigung zum Freigeben einer Elastic IP-Adresse	Write	elastic-ip	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	
				ec2:Region	
ReleaseHosts	Gewährt die Berechtigung zur Freigabe eines oder mehrerer On-Demand Dedicated Hosts	Schreiben	dedicated-host*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ReleaseIpamPoolAllocation	Gewährt die Berechtigung zum Freigeben einer Zuteilung innerhalb eines Amazon VPC IP Address Manager (IPAM)-Pools	Schreiben	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ReplaceIamInstanceProfileAssociation	Gewährt die Berechtigung zum Ersetzen eines IAM-Instance-Profils für eine Instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:NewInstanceProfile ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
ReplaceNetworkAclAssociation	Gewährt die Berechtigung zum Ändern der Netzwerk-ACL, mit der ein Subnetz verknüpft ist	Write	network-acl*	aws:ResourceTag/${TagKey} ec2:NetworkAclID ec2:ResourceTag/${TagKey} ec2:Vpc	
			subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
ReplaceNetworkAclEntry	Gewährt die Berechtigung zum Ersetzen eines Eintrags (Regel) in einer Netzwerk-ACL	Write	network-acl*	aws:ResourceTag/${TagKey} ec2:NetworkAclID ec2:ResourceTag/${TagKey} ec2:Vpc	
				ec2:Region	
ReplaceRoute	Gewährt die Berechtigung zum Ersetzen einer Route innerhalb einer Routing-Tabelle in einer VPC	Write	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ReplaceRouteTableAssociation	Gewährt die Berechtigung zum Ändern der Routing-Tabelle, die einem Subnetz zugeordnet ist	Write	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
			internet-gateway	aws:ResourceTag/${TagKey} ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	
			ipv4pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			ipv6pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
			vpn-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	
ReplaceTransitGatewayRoute	Gewährt die Berechtigung, eine Route in der Routing-Tabelle für ein Transit-Gateway zu ersetzen	Schreiben	transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ReplaceVpnTunnel	Gewährt die Berechtigung zum Ersetzen eines VPN-Tunnels	Schreiben	vpn-connection*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ReportInstanceStatus	Gewährt die Berechtigung, Feedback zum Status einer Instance zu übermitteln	Write		ec2:Region	
RequestSpotFleet	Gewährt die Berechtigung zum Erstellen einer Spot-Flottenanforderung	Write	spot-fleet-request*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			image	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			key-pair	aws:ResourceTag/${TagKey} ec2:KeyPairName ec2:KeyPairType ec2:ResourceTag/${TagKey}	
			launch-template	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			placement-group	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			snapshot	aws:ResourceTag/${TagKey} ec2:OutpostArn ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:SourceOutpostArn ec2:VolumeSize	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	
RequestSpotInstances	Gewährt die Berechtigung zum Erstellen einer Spot-Instance-Anforderung	Write	spot-instances-request*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			image	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			key-pair	aws:ResourceTag/${TagKey} ec2:KeyPairName ec2:KeyPairType ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			network-interface	aws:ResourceTag/${TagKey} ec2:AuthorizedUser ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:Permission ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			placement-group	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			snapshot	aws:ResourceTag/${TagKey} ec2:OutpostArn ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:SourceOutpostArn ec2:VolumeSize	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ResetAddressAttribute	Gewährt die Berechtigung zum Zurücksetzen des Attributs der angegebenen IP-Adresse	Schreiben	elastic-ip*	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Attribute ec2:Attribute/${AttributeName} ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ResetEbsDefaultKmsKeyId	Erteilt die Berechtigung, den Standard-Kundenhauptschlüssel (CMK) für die EBS-Verschlüsselung für Ihr Konto zurückzusetzen, sodass der von -verwaltete CMK für EBS verwendet werden kann AWS	Schreiben		ec2:Region	
ResetFpgaImageAttribute	Gewährt die Berechtigung, ein Attribut eines Amazon FPGA-Image (AFI) auf den Standardwert zurückzusetzen	Write	fpga-image*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:Owner ec2:Public ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ResetImageAttribute	Gewährt die Berechtigung, ein Attribut eines Amazon Machine Image (AMI) auf seinen Standardwert zurückzusetzen	Write	image*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ResetInstanceAttribute	Gewährt die Berechtigung, ein Attribut einer Instance auf seinen Standardwert zurückzusetzen	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ResetNetworkInterfaceAttribute	Gewährt die Berechtigung zum Zurücksetzen eines Attributs einer Netzwerkschnittstelle	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ResetSnapshotAttribute	Gewährt die Berechtigung zum Zurücksetzen von Berechtigungseinstellungen für einen Snapshot	Berechtigungsverwaltung	snapshot*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RestoreAddressToClassic	Gewährt die Berechtigung, eine Elastic IP-Adresse, die zuvor zur EC2-VPC-Plattform verschoben wurde, auf der EC2-Classic-Plattform wieder herzustellen	Schreiben		ec2:Region	
RestoreImageFromRecycleBin	Erteilt die Berechtigung, ein Amazon Machine Image (AMI) aus einem Papierkorb wiederherzustellen	Schreiben	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RestoreManagedPrefixListVersion	Gewährt die Berechtigung zum Wiederherstellen der Einträge aus einer früheren Version einer verwalteten Präfixliste in eine neue Version der Präfixliste	Schreiben	prefix-list*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RestoreSnapshotFromRecycleBin	Gewährt die Berechtigung zum Wiederherstellen eines Amazon-EBS-Snapshots aus dem Recycle Bin	Schreiben	snapshot*	aws:ResourceTag/${TagKey} ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RestoreSnapshotTier	Gewährt die Berechtigung, einen archivierten Amazon-EBS-Snapshot zur vorübergehenden oder dauerhaften Verwendung wiederherzustellen oder den Wiederherstellungszeitraum oder den Wiederherstellungstyp für einen Snapshot zu ändern, der zuvor vorübergehend wiederhergestellt wurde	Schreiben	snapshot*	aws:ResourceTag/${TagKey} ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RevokeClientVpnIngress	Gewährt die Berechtigung zum Entfernen einer Autorisierungsregel für eingehenden Datenverkehr von einem Client-VPN-Endpunkt	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RevokeSecurityGroupEgress	Gewährt die Berechtigung zum Entfernen einer oder mehrerer Regeln für ausgehenden Datenverkehr aus einer VPC-Sicherheitsgruppe	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
				ec2:Region	
RevokeSecurityGroupIngress	Gewährt die Berechtigung zum Entfernen einer oder mehrerer Regeln für eingehenden Datenverkehr aus einer Sicherheitsgruppe	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RunInstances	Gewährt die Berechtigung zum Starten einer oder mehrerer Instances	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	ec2:CreateTags iam:PassRole ssm:GetParameters

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			instance*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:InstanceType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:RootDeviceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Tenancy	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			network-interface*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AssociatePublicIpAddress ec2:AuthorizedService ec2:AvailabilityZone ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:NetworkInterfaceID ec2:Subnet	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Vpc	
			security-group*	aws:ResourceTag/${TagKey} ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			capacity-reservation	aws:ResourceTag/${TagKey} ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ResourceTag/${TagKey}	
			elastic-gpu	aws:ResourceTag/${TagKey} ec2:ElasticGpuType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			elastic-inference		
			group		
			key-pair	aws:ResourceTag/${TagKey} ec2:IsLaunchTemplateResource ec2:KeyPairName ec2:KeyPairType ec2:LaunchTemplate ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			launch-template	aws:ResourceTag/${TagKey} ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ResourceTag/${TagKey}	
			license-configuration		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			placement-group	aws:ResourceTag/${TagKey} ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			snapshot	aws:ResourceTag/${TagKey} ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			volume	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:Encrypted ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ParentSnapshot ec2:VolumeID ec2:VolumeIops ec2:VolumeSize	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	
	SZENARIO: EC2-Classic-EBS		image* instance* security-group* volume* key-pair placement-group snapshot		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	SZENARIO: EC2-Classic-InstanceStore		image* instance* security-group* key-pair placement-group snapshot		
	SZENARIO: EC2-VPC-EBS		image* instance* network-interface* security-group* volume* key-pair placement-group snapshot		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	SZENARIO: EC2-VPC-EBS-Subnet		image* instance* network-interface* security-group* subnet* volume* key-pair placement-group snapshot		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	SZENARIO: EC2-VPC-InstanceStore		image* instance* network-interface* security-group* key-pair placement-group snapshot		
	SZENARIO: EC2-VPC-InstanceStore-Subnet		image* instance* network-interface* security-group* subnet* key-pair placement-group snapshot		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RunScheduledInstances	Gewährt die Berechtigung zum Starten einer oder mehrerer geplanter Instances	Write		ec2:Region	
SearchLocalGatewayRoutes	Gewährt die Berechtigung, in der Routing-Tabelle eines lokalen Gateways nach Routen zu suchen	List	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
SearchTransitGatewayMulticastGroups	Gewährt die Berechtigung zum Suchen nach Gruppen, Quellen und Mitgliedern in einer Transit-Gateway-Multicast-Domain	List	transit-gateway-multicast-domain*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SearchTransitGatewayRoutes	Gewährt die Berechtigung zum Suchen nach Routen in der Routing-Tabelle eines Transit-Gateways	List	transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SendDiagnosticInterrupt	Gewährt die Berechtigung zum Senden eines Diagnose-Interrupts an eine Amazon EC2-Instance	Schreiben	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SendSpotInstanceInterruptions [nur Berechtigung]	Gewährt die Berechtigung zum Unterbrechen einer Spot-Instance	Schreiben	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartInstances	Gewährt die Berechtigung zum Starten einer gestoppten Instance	Schreiben	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceID ec2:InstanceMarketType ec2:InstanceProfile ec2:InstanceType ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
			license-configuration		
				ec2:Region	
StartNetworkInsightsAccessScopeAnalysis	Gewährt die Berechtigung zum Starten einer Analyse des Netzwerkzugriffs-Bereichs	Schreiben	network-insights-access-scope*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			network-insights-access-scope-analysis*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	
StartNetworkInsightsAnalysis	Gewährt die Berechtigung, die Analyse eines angegebenen Pfads zu starten	Write	network-insights-analysis*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			network-insights-path*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartVpcEndpointServicePrivateDnsVerification	Gewährt die Berechtigung zum Starten des privaten DNS-Überprüfungsprozesses für einen VPC-Endpunkt-Service	Write	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopInstances	Gewährt die Berechtigung zum Beenden einer Amazon EBS-gestützten Instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Terminate ClientVpn Connections	Gewährt die Berechtigung zum Beenden von aktiven Client-VPN-Endpunktverbindungen	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Terminate Instances	Gewährt die Berechtigung zum Herunterfahren einer oder mehrerer Instances	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UnassignIpv6Addresses	Gewährt die Berechtigung zum Aufheben der Zuweisung einer oder mehrerer IPv6-Adressen zu einer Netzwerkschnittstelle	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UnassignPrivateIpAddresses	Gewährt die Berechtigung zum Aufheben der Zuweisung einer oder mehrerer sekundärer privater IP-Adressen zu einer Netzwerkschnittstelle	Schreiben	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	
UnassignPrivateNatGatewayAddress	Gewährt die Berechtigung zum Aufheben der Zuweisung sekundärer privater IPv4-Adressen zu einem privaten NAT-Gateway	Schreiben	natgateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UnlockSnapshot	Gewährt die Berechtigung, einen Snapshot zu entsperren, der im Governance-Modus oder im Compliance-Modus gesperrt ist, während er sich noch in der Abkühlungsphase befindet	Schreiben	snapshot*	aws:ResourceTag/${TagKey} ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotCoolOffPeriod ec2:SnapshotID ec2:SnapshotLockDuration ec2:SnapshotTime ec2:VolumeSize	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UnmonitorInstances	Gewährt die Berechtigung zum Deaktivieren der detaillierten Überwachung für eine ausgeführte Instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateSecurityGroupRuleDescriptionsEgress	Gewährt die Berechtigung zum Aktualisieren von Beschreibungen für eine oder mehrere Regeln für ausgehenden Datenverkehr in einer VPC-Sicherheitsgruppe	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
				ec2:Region	
UpdateSecurityGroupRuleDescriptionsIngress	Gewährt die Berechtigung, Beschreibungen für eine oder mehrere Regeln für eingehenden Datenverkehr in einer Sicherheitsgruppe zu aktualisieren	Schreiben	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
				ec2:Region	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
WithdrawByoipCidr	Erteilt die Erlaubnis, die Werbung für einen Adressbereich zu beenden, der für die Nutzung AWS über Bring Your Own IP-Adressen (BYOIP) bereitgestellt wurde	Schreiben		ec2:Region	

Von Amazon EC2 definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
elastic-ip	`arn:${Partition}:ec2:${Region}:${Account}:elastic-ip/${AllocationId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AllocationId ec2:Attribute ec2:Attribute/${AttributeName}

Ressourcentypen	ARN	Bedingungsschlüssel
		ec2:Domain ec2:PublicIpAddress ec2:Region ec2:ResourceTag/${TagKey}
capacity-reservation-fleet	arn:${Partition}:ec2:${Region}:${Account}:capacity-reservation-fleet/${CapacityReservationFleetId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
capacity-reservation	`arn:${Partition}:ec2:${Region}:${Account}:capacity-reservation/${CapacityReservationId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:CapacityReservationFleet ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
carrier-gateway	arn:${Partition}:ec2:${Region}:${Account}:carrier-gateway/${CarrierGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:Vpc
certificate	arn:${Partition}:acm:${Region}:${Account}:certificate/${CertificateId}	

Ressourcentypen	ARN	Bedingungsschlüssel
client-vpn-endpoint	`arn:${Partition}:ec2:${Region}:${Account}:client-vpn-endpoint/${ClientVpnEndpointId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:Region ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn

Ressourcentypen	ARN	Bedingungsschlüssel
customer-gateway	`arn:${Partition}:ec2:${Region}:${Account}:customer-gateway/${CustomerGatewayId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
dedicated-host	`arn:${Partition}:ec2:${Region}:${Account}:dedicated-host/${DedicatedHostId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:AutoPlacement ec2:AvailabilityZone ec2:HostRecovery ec2:InstanceType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Quantity ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
dhcp-options	arn:${Partition}:ec2:${Region}:${Account}:dhcp-options/${DhcpOptionsId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:DhcpOptionsID ec2:Region ec2:ResourceTag/${TagKey}
egress-only-internet-gateway	arn:${Partition}:ec2:${Region}:${Account}:egress-only-internet-gateway/${EgressOnlyInternetGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
elastic-gpu	arn:${Partition}:ec2:${Region}:${Account}:elastic-gpu/${ElasticGpuId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ElasticGpuType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:ResourceTag/${TagKey}
elastic-inference	arn:${Partition}:elastic-inference:${Region}:${Account}:elastic-inference-accelerator/${AcceleratorId}	
export-image-task	arn:${Partition}:ec2:${Region}:${Account}:export-image-task/${ExportImageTaskId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
export-instance-task	arn:${Partition}:ec2:${Region}:${Account}:export-instance-task/${ExportTaskId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
fleet	arn:${Partition}:ec2:${Region}:${Account}:fleet/${FleetId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
fpga-image	arn:${Partition}:ec2:${Region}:${Account}:fpga-image/${FpgaImageId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Owner ec2:Public ec2:Region ec2:ResourceTag/${TagKey}
host-reservation	arn:${Partition}:ec2:${Region}:${Account}:host-reservation/${HostReservationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
image	`arn:${Partition}:ec2:${Region}::image/${ImageId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:ImageID ec2:ImageType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Owner ec2:Public ec2:Region ec2:ResourceTag/${TagKey} ec2:RootDeviceType

Ressourcentypen	ARN	Bedingungsschlüssel
import-image-task	arn:${Partition}:ec2:${Region}:${Account}:import-image-task/${ImportImageTaskId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
import-snapshot-task	arn:${Partition}:ec2:${Region}:${Account}:import-snapshot-task/${ImportSnapshotTaskId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
instance-connect-endpoint	`arn:${Partition}:ec2:${Region}:${Account}:instance-connect-endpoint/${InstanceConnectEndpointId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey} ec2:SubnetID
instance-event-window	`arn:${Partition}:ec2:${Region}:${Account}:instance-event-window/${InstanceEventWindowId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
instance	`arn:${Partition}:ec2:${Region}:${Account}:instance/${InstanceId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:IsLaunchTemplateResource ec2:LaunchTemplate

Ressourcentypen	ARN	Bedingungsschlüssel
		ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:NewInstanceProfile ec2:PlacementGroup ec2:ProductCode ec2:Region ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy

Ressourcentypen	ARN	Bedingungsschlüssel
internet-gateway	arn:${Partition}:ec2:${Region}:${Account}:internet-gateway/${InternetGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:InternetGatewayID ec2:Region ec2:ResourceTag/${TagKey}
ipam	arn:${Partition}:ec2::${Account}:ipam/${IpamId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
ipam-pool	`arn:${Partition}:ec2::${Account}:ipam-pool/${IpamPoolId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
ipam-resource-discovery-association	`arn:${Partition}:ec2::${Account}:ipam-resource-discovery-association/${IpamResourceDiscoveryAssociationId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
ipam-resource-discovery	arn:${Partition}:ec2::${Account}:ipam-resource-discovery/${IpamResourceDiscoveryId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
ipam-scope	arn:${Partition}:ec2::${Account}:ipam-scope/${IpamScopeId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
coip-pool	arn:${Partition}:ec2:${Region}:${Account}:coip-pool/${Ipv4PoolCoipId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
ipv4pool-ec2	arn:${Partition}:ec2:${Region}:${Account}:ipv4pool-ec2/${Ipv4PoolEc2Id}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
ipv6pool-ec2	arn:${Partition}:ec2:${Region}:${Account}:ipv6pool-ec2/${Ipv6PoolEc2Id}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
key-pair	`arn:${Partition}:ec2:${Region}:${Account}:key-pair/${KeyPairName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:IsLaunchTemplateResource ec2:KeyPairName ec2:KeyPairType ec2:LaunchTemplate ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
launch-template	arn:${Partition}:ec2:${Region}:${Account}:launch-template/${LaunchTemplateId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:ResourceTag/${TagKey}
license-configuration	arn:${Partition}:license-manager:${Region}:${Account}:license-configuration:${LicenseConfigurationId}	

Ressourcentypen	ARN	Bedingungsschlüssel
local-gateway	arn:${Partition}:ec2:${Region}:${Account}:local-gateway/${LocalGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
local-gateway-route-table-virtual-interface-group-association	arn:${Partition}:ec2:${Region}:${Account}:local-gateway-route-table-virtual-interface-group-association/${LocalGatewayRouteTableVirtualInterfaceGroupAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
local-gateway-route-table-vpc-association	arn:${Partition}:ec2:${Region}:${Account}:local-gateway-route-table-vpc-association/${LocalGatewayRouteTableVpcAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
local-gateway-route-table	arn:${Partition}:ec2:${Region}:${Account}:local-gateway-route-table/${LocalGatewayRoutetableId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
local-gateway-virtual-interface-group	arn:${Partition}:ec2:${Region}:${Account}:local-gateway-virtual-interface-group/${LocalGatewayVirtualInterfaceGroupId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
local-gateway-virtual-interface	arn:${Partition}:ec2:${Region}:${Account}:local-gateway-virtual-interface/${LocalGatewayVirtualInterfaceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
natgateway	arn:${Partition}:ec2:${Region}:${Account}:natgateway/${NatGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
network-acl	arn:${Partition}:ec2:${Region}:${Account}:network-acl/${NaclId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:NetworkAclID ec2:Region ec2:ResourceTag/${TagKey} ec2:Vpc

Ressourcentypen	ARN	Bedingungsschlüssel
network-insights-access-scope-analysis	arn:${Partition}:ec2:${Region}:${Account}:network-insights-access-scope-analysis/${NetworkInsightsAccessScopeAnalysisId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
network-insights-access-scope	arn:${Partition}:ec2:${Region}:${Account}:network-insights-access-scope/${NetworkInsightsAccessScopeId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
network-insights-analysis	arn:${Partition}:ec2:${Region}:${Account}:network-insights-analysis/${NetworkInsightsAnalysisId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
network-insights-path	arn:${Partition}:ec2:${Region}:${Account}:network-insights-path/${NetworkInsightsPathId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
network-interface	arn:${Partition}:ec2:${Region}:${Account}:network-interface/${NetworkInterfaceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AssociatePublicIpAddress ec2:Attribute ec2:Attribute/${AttributeName} ec2:AuthorizedService ec2:AuthorizedUser ec2:AvailabilityZone ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:NetworkInterfaceID ec2:Permission ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
		ec2:Subnet ec2:Vpc
placement-group	arn:${Partition}:ec2:${Region}:${Account}:placement-group/${PlacementGroupName}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
prefix-list	arn:${Partition}:ec2:${Region}:${Account}:prefix-list/${PrefixListId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
replace-root-volume-task	arn:${Partition}:ec2:${Region}:${Account}:replace-root-volume-task/${ReplaceRootVolumeTaskId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
reserved-instances	arn:${Partition}:ec2:${Region}:${Account}:reserved-instances/${ReservationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:InstanceType ec2:Region ec2:ReservedInstancesOfferingType ec2:ResourceTag/${TagKey} ec2:Tenancy
group	arn:${Partition}:resource-groups:${Region}:${Account}:group/${GroupName}	
role	arn:${Partition}:iam::${Account}:role/${RoleNameWithPath}	

Ressourcentypen	ARN	Bedingungsschlüssel
route-table	`arn:${Partition}:ec2:${Region}:${Account}:route-table/${RouteTableId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc

Ressourcentypen	ARN	Bedingungsschlüssel
security-group	`arn:${Partition}:ec2:${Region}:${Account}:security-group/${SecurityGroupId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc

Ressourcentypen	ARN	Bedingungsschlüssel
security-group-rule	`arn:${Partition}:ec2:${Region}:${Account}:security-group-rule/${SecurityGroupRuleId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
snapshot	`arn:${Partition}:ec2:${Region}::snapshot/${SnapshotId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Add/group ec2:Add/userId ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:Encrypted ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:OutpostArn ec2:Owner ec2:ParentVolume ec2:Region ec2:Remove/group ec2:Remove/userId

Ressource ntypen	ARN	Bedingungsschlüssel
		ec2:ResourceTag/${TagKey} ec2:SnapshotCoolOffPeriod ec2:SnapshotID ec2:SnapshotLockDuration ec2:SnapshotTime ec2:SourceOutpostArn ec2:VolumeSize
spot-fleet-request	arn:${Partition}:ec2:${Region}:${Account}:spot-fleet-request/${SpotFleetRequestId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
spot-instances-request	arn:${Partition}:ec2:${Region}:${Account}:spot-instances-request/${SpotInstanceRequestId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
subnet-cidr-reservation	arn:${Partition}:ec2:${Region}:${Account}:subnet-cidr-reservation/${SubnetCidrReservationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
subnet	`arn:${Partition}:ec2:${Region}:${Account}:subnet/${SubnetId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc

Ressourcentypen	ARN	Bedingungsschlüssel
traffic-mirror-filter	`arn:${Partition}:ec2:${Region}:${Account}:traffic-mirror-filter/${TrafficMirrorFilterId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
traffic-mirror-filter-rule	`arn:${Partition}:ec2:${Region}:${Account}:traffic-mirror-filter-rule/${TrafficMirrorFilterRuleId}`	ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region

Ressourcentypen	ARN	Bedingungsschlüssel
traffic-mirror-session	arn:${Partition}:ec2:${Region}:${Account}:traffic-mirror-session/${TrafficMirrorSessionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
traffic-mirror-target	arn:${Partition}:ec2:${Region}:${Account}:traffic-mirror-target/${TrafficMirrorTargetId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
transit-gateway-attachment	arn:${Partition}:ec2:${Region}:${Account}:transit-gateway-attachment/${TransitGatewayAttachmentId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId
transit-gateway-connect-peer	arn:${Partition}:ec2:${Region}:${Account}:transit-gateway-connect-peer/${TransitGatewayConnectPeerId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey} ec2:transitGatewayConnectPeerId

Ressourcentypen	ARN	Bedingungsschlüssel
transit-gateway	`arn:${Partition}:ec2:${Region}:${Account}:transit-gateway/${TransitGatewayId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey} ec2:transitGatewayId
transit-gateway-multicast-domain	`arn:${Partition}:ec2:${Region}:${Account}:transit-gateway-multicast-domain/${TransitGatewayMulticastDomainId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId

Ressourcentypen	ARN	Bedingungsschlüssel
transit-gateway-policy-table	arn:${Partition}:ec2:${Region}:${Account}:transit-gateway-policy-table/${TransitGatewayPolicyTableId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey} ec2:transitGatewayPolicyTableId
transit-gateway-route-table-announcement	arn:${Partition}:ec2:${Region}:${Account}:transit-gateway-route-table-announcement/${TransitGatewayRouteTableAnnouncementId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableAnnouncementId

Ressourcentypen	ARN	Bedingungsschlüssel
transit-gateway-route-table	arn:${Partition}:ec2:${Region}:${Account}:transit-gateway-route-table/${TransitGatewayRouteTableId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId
verified-access-endpoint	arn:${Partition}:ec2:${Region}:${Account}:verified-access-endpoint/${VerifiedAccessEndpointId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
verified-access-group	arn:${Partition}:ec2:${Region}:${Account}:verified-access-group/${VerifiedAccessGroupId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
verified-access-instance	arn:${Partition}:ec2:${Region}:${Account}:verified-access-instance/${VerifiedAccessInstanceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
verified-access-policy	arn:${Partition}:ec2:${Region}:${Account}:verified-access-policy/${VerifiedAccessPolicyId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
verified-access-trust-provider	`arn:${Partition}:ec2:${Region}:${Account}:verified-access-trust-provider/${VerifiedAccessTrustProviderId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
volume	`arn:${Partition}:ec2:${Region}:${Account}:volume/${VolumeId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:Encrypted ec2:IsLaunchTemplateResource ec2:KmsKeyId ec2:LaunchTemplate ec2:ParentSnapshot ec2:Region ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput

Ressourcentypen	ARN	Bedingungsschlüssel
		ec2:VolumeType
vpc-endpoint-connection	arn:${Partition}:ec2:${Region}:${Account}:vpc-endpoint-connection/${VpcEndpointConnectionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
vpc-endpoint	arn:${Partition}:ec2:${Region}:${Account}:vpc-endpoint/${VpcEndpointId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey} ec2:VpceServiceName ec2:VpceServiceOwner

Ressourcentypen	ARN	Bedingungsschlüssel
vpc-endpoint-service	arn:${Partition}:ec2:${Region}:${Account}:vpc-endpoint-service/${VpcEndpointServiceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey} ec2:VpceServicePrivateDnsName
vpc-endpoint-service-permission	arn:${Partition}:ec2:${Region}:${Account}:vpc-endpoint-service-permission/${VpcEndpointServicePermissionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
vpc-flow-log	arn:${Partition}:ec2:${Region}:${Account}:vpc-flow-log/${VpcFlowLogId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
vpc	arn:${Partition}:ec2:${Region}:${Account}:vpc/${VpcId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:Region ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID

Ressourcentypen	ARN	Bedingungsschlüssel
vpc-peering-connection	arn:${Partition}:ec2:${Region}:${Account}:vpc-peering-connection/${VpcPeeringConnectionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AccepterVpc ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:RequesterVpc ec2:ResourceTag/${TagKey} ec2:VpcPeeringConnectionID
vpn-connection-device-type	arn:${Partition}:ec2:${Region}:${Account}:vpn-connection-device-type/${VpnConnectionDeviceTypeId}	ec2:Region

Ressourcentypen	ARN	Bedingungsschlüssel
vpn-connection	arn:${Partition}:ec2:${Region}:${Account}:vpn-connection/${VpnConnectionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:AuthenticationType ec2:DPDTimeoutSeconds ec2:GatewayType ec2:IKEVersions ec2:InsideTunnelCidr ec2:InsideTunnelIpv6Cidr ec2:Phase1DHGroup ec2:Phase1EncryptionAlgorithms ec2:Phase1IntegrityAlgorithms ec2:Phase1LifetimeSeconds

Ressourcentypen	ARN	Bedingungsschlüssel
		ec2:Phase2DHGroup ec2:Phase2EncryptionAlgorithms ec2:Phase2IntegrityAlgorithms ec2:Phase2LifetimeSeconds ec2:Region ec2:RekeyFuzzPercentage ec2:RekeyMarginTimeSeconds ec2:ReplayWindowSizePackets ec2:ResourceTag/${TagKey} ec2:RoutingType

Ressourcentypen	ARN	Bedingungsschlüssel
vpn-gateway	`arn:${Partition}:ec2:${Region}:${Account}:vpn-gateway/${VpnGatewayId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon EC2

Amazon EC2 definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wertepaaren, die in der Anforderung zulässig sind	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paar einer Ressource	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach Liste von Tag-Schlüsseln, die in der Anforderung zulässig sind	ArrayOfString

Bedingungsschlüssel	Beschreibung	Typ
ec2:AccepterVpc	Filtert den Zugriff nach ARN einer Annehmer-VPC in einer VPC-Peering-Verbindung	ARN
ec2:Add/group	Filtert den Zugriff nach der Gruppe, die einem Snapshot hinzugefügt wird	String
ec2:Add/userId	Filtert den Zugriff nach der Konto-ID, die zu einem Snapshot hinzugefügt wird	String
ec2:AllocationId	Filtert den Zugriff nach der Zuordnungs-ID der elastischen IP-Adresse	String
ec2:AssociatePublicIpAddress	Filtert den Zugriff danach, ob der Benutzer der Instance eine öffentliche IP-Adresse zuordnen möchte.	Bool
ec2:Attribute	Filtert den Zugriff nach einem Attribut einer Ressource	String
ec2:Attribute/${AttributeName}	Filtert den Zugriff nach einem Attribut, das für eine Ressource festgelegt wurde	Zeichenfolge
ec2:AuthenticationType	Filtert den Zugriff nach Authentifizierungstyp für die VPN-Tunnel-Endpunkte	String
ec2:AuthorizedService	Filtert den Zugriff nach dem AWS Dienst, der über die Berechtigung zur Nutzung einer Ressource verfügt	String
ec2:AuthorizedUser	Filtert den Zugriff nach IAM-Prinzipalen, die über die Berechtigung zur Verwendung einer Ressource verfügen	Zeichenfolge
ec2:AutoPlacement	Filtert den Zugriff nach Eigenschaften der automatischen Platzierung eines Dedicated Hosts	String
ec2:AvailabilityZone	Filtert den Zugriff nach dem Namen einer Availability Zone in einem AWS-Region	String

Bedingungsschlüssel	Beschreibung	Typ
ec2:CapacityReservationFleet	Filtert den Zugriff nach ARN der Flotte zu Kapazitätsreservierungen	ARN
ec2:ClientRootCertificateChainArn	Filtert den Zugriff nach dem ARN der Client-Stammzertifikat-Kette	ARN
ec2:CloudwatchLogGroupArn	Filtert den Zugriff nach dem ARN der Protokollgruppe CloudWatch Logs	ARN
ec2:CloudwatchLogStreamArn	Filtert den Zugriff nach dem ARN des CloudWatch Log-Streams	ARN
ec2:CreateAction	Filtert den Zugriff nach Name einer ressourcenerstellenden API-Aktion	Zeichenfolge
ec2:DPDTimeoutSeconds	Filtert den Zugriff nach der Dauer, nach der eine DPD-Zeitüberschreitung in einem VPN-Tunnel auftritt	Numerischer Wert
ec2:DhcpOptionsID	Filtert den Zugriff nach der ID eines Options-Set des Dynamic Host Configuration Protocol (DHCP)	String
ec2:DirectoryArn	Filtert den Zugriff nach dem ARN des Verzeichnisses	ARN
ec2:Domain	Filtert den Zugriff nach der Domain der elastischen IP-Adresse	String
ec2:EbsOptimized	Filtert den Zugriff danach, ob die Instance zur EBS-Optimierung fähig ist	Bool
ec2:ElasticGpuType	Filtert den Zugriff nach Typ des Elastic Graphics Accelerators	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
ec2:Encrypted	Filtert den Zugriff danach, ob das EBS-Volume verschlüsselt ist	Bool
ec2:FisActionId	Filtert den Zugriff nach der ID einer AWS FIS-Aktion	String
ec2:FisTargetArns	Filtert den Zugriff nach dem ARN eines AWS FIS-Ziels	ArrayOfARN
ec2:GatewayType	Filtert den Zugriff nach dem Gateway-Typ für einen VPN-Endpunkt auf der AWS Seite einer VPN-Verbindung	String
ec2:HostRecovery	Filtert den Zugriff danach, ob die Hostwiederherstellung für einen Dedicated Host aktiviert ist	Zeichenfolge
ec2:IKEVersions	Filtert den Zugriff nach IKE-Versionen (Internet Key Exchange), die für einen VPN-Tunnel zulässig sind	ArrayOfString
ec2:ImageID	Filtert den Zugriff nach der ID eines Images	String
ec2:ImageType	Filtert den Zugriff nach Image-Typ (Maschine, Aki oder Ari)	Zeichenfolge
ec2:InsideTunnelCidr	Filtert den Zugriff nach Bereich der internen IP-Adressen für einen VPN-Tunnel	String
ec2:InsideTunnelIpv6Cidr	Filtert den Zugriff nach einem Bereich der internen IPv6-Adressen für einen VPN-Tunnel	String
ec2:InstanceAutoRecovery	Filtert den Zugriff danach, ob der Instance-Typ die automatische Wiederherstellung unterstützt	String
ec2:InstanceID	Filtert den Zugriff nach der ID einer Instance	String
ec2:InstanceMarketType	Filtert den Zugriff nach Markt oder Kaufoption einer (On-Demand- oder Spot-)Instance	String

Bedingungsschlüssel	Beschreibung	Typ
ec2:InstanceMetadataTags	Filtert den Zugriff danach, ob die Instance den Zugriff auf Instance-Tags aus den Instance-Metadaten ermöglicht	String
ec2:InstanceProfile	Filtert den Zugriff nach ARN eines Instance-Profils	ARN
ec2:InstanceType	Filtert den Zugriff nach Instance-Typ	String
ec2:InternetGatewayID	Filtert den Zugriff nach der ID eines Internet-Gateways	String
ec2:Ipv4IpamPoolId	Filtert den Zugriff nach der ID eines IPAM-Pools, der für die IPv4-CIDR-Blockzuweisung vorgesehen ist	String
ec2:Ipv6IpamPoolId	Filtert den Zugriff nach der ID eines IPAM-Pools, der für die IPv6-CIDR-Blockzuweisung vorgesehen ist	String
ec2:IsLaunchTemplateResource	Filtert den Zugriff danach, ob Benutzer Ressourcen überschreiben können, die in der Startvorlage angegeben sind	Bool
ec2:KeyPairName	Filtert den Zugriff nach dem Namen des Schlüsselpaars	String
ec2:KeyPairType	Filtert den Zugriff nach dem Typ des Schlüsselpaars	String
ec2:KmsKeyId	Filtert den Zugriff anhand der ID eines AWS KMS-Schlüssels, der in der Anfrage angegeben wurde	String
ec2:LaunchTemplate	Filtert den Zugriff nach ARN einer Startvorlage	ARN

Bedingungsschlüssel	Beschreibung	Typ
ec2:MetadataHttpEndpoint	Filtert den Zugriff danach, ob der HTTP-Endpunkt für den Instance-Metadaten-Service aktiviert ist	Zeichenfolge
ec2:MetadataHttpPutResponseHopLimit	Filtert den Zugriff nach zulässiger Anzahl von Hops beim Aufruf des Instance-Metadaten-Service	Numerischer Wert
ec2:MetadataHttpTokens	Filtert den Zugriff danach, ob beim Aufruf des Instance-Metadaten-Service Token erforderlich sind (optional oder erforderlich)	String
ec2:NetworkAclID	Filtert den Zugriff nach der ID einer Netzwerk-Zugriffssteuerungsliste (ACL)	String
ec2:NetworkInterfaceID	Filtert den Zugriff nach der ID einer Elastic-Network-Schnittstelle	String
ec2:NewInstanceProfile	Filtert den Zugriff durch den ARN des angehängten Instance-Profils	ARN
ec2:OutpostArn	Filtert den Zugriff nach ARN des Outposts	ARN
ec2:Owner	Filtert den Zugriff durch den Eigentümer der Ressource (Amazon, aws-marketplace oder eine AWS-Konto ID)	String
ec2:ParentSnapshot	Filtert den Zugriff nach ARN des übergeordneten Snapshots	ARN
ec2:ParentVolume	Filtert den Zugriff nach ARN des übergeordneten Volumes, aus dem der Snapshot erstellt wurde	ARN
ec2:Permission	Filtert den Zugriff nach Berechtigungstyp für eine Ressource (INSTANCE-ATTACH oder EIP-ASSOCIATE)	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
ec2:Phase1DHGroup	Filtert den Zugriff nach Diffie-Hellman-Gruppennummern, die für einen VPN-Tunnel für die IKE-Verhandlungen der Phase 1 zulässig sind	ArrayOfString
ec2:Phase1EncryptionAlgorithms	Filtert den Zugriff durch die Verschlüsselungsalgorithmen, die für einen VPN-Tunnel für die IKE-Verhandlungen der Phase 1 zulässig sind	ArrayOfString
ec2:Phase1IntegrityAlgorithms	Filtert den Zugriff nach Integritätsalgorithmen, die für einen VPN-Tunnel für die IKE-Verhandlungen der Phase 1 zulässig sind	ArrayOfString
ec2:Phase1LifetimeSeconds	Filtert den Zugriff nach Lebensdauer in Sekunden für Phase 1 der IKE-Verhandlungen für einen VPN-Tunnel	Numerischer Wert
ec2:Phase2DHGroup	Filtert den Zugriff nach Diffie-Hellman-Gruppennummern, die für einen VPN-Tunnel für die IKE-Verhandlungen der Phase 2 zulässig sind	ArrayOfString
ec2:Phase2EncryptionAlgorithms	Filtert den Zugriff nach Verschlüsselungsalgorithmen, die für einen VPN-Tunnel für die IKE-Verhandlungen der Phase 2 zulässig sind	ArrayOfString
ec2:Phase2IntegrityAlgorithms	Filtert den Zugriff nach Integritätsalgorithmen, die für den VPN-Tunnel für die IKE-Verhandlungen der Phase 2 zulässig sind	ArrayOfString
ec2:Phase2LifetimeSeconds	Filtert den Zugriff nach Lebensdauer in Sekunden für Phase 2 der IKE-Verhandlungen für einen VPN-Tunnel	Numerischer Wert
ec2:PlacementGroup	Filtert den Zugriff nach ARN der Platzierungsgruppe	ARN

Bedingungsschlüssel	Beschreibung	Typ
ec2:PlacementGroupName	Filtert den Zugriff nach dem Namen einer Platzierungsgruppe	String
ec2:PlacementGroupStrategy	Filtert den Zugriff nach Instance-Platzierungsstrategie, die von der Platzierungsgruppe (Cluster, Spread oder Partition) verwendet wird	String
ec2:ProductCode	Filtert den Zugriff nach dem Produktcode, der dem AMI zugeordnet ist	Zeichenfolge
ec2:Public	Filtert den Zugriff danach, ob das Image über öffentliche Startberechtigungen verfügt	Bool
ec2:PublicIpAddress	Filtert den Zugriff nach öffentlicher IP-Adresse	String
ec2:Quantity	Filtert den Zugriff nach Anzahl von Dedicated Hosts in einer Anforderung	Numerischer Wert
ec2:Region	Filtert den Zugriff nach dem Namen des AWS-Region	String
ec2:RekeyFuzzPercentage	Filtert den Zugriff nach Prozentsatz der Erhöhung des Rekey-Fensters (bestimmt durch die Rekey-Zeitspanne), innerhalb dessen die Rekey-Zeit für einen VPN-Tunnel nach dem Zufallsprinzip ausgewählt wird	Numerischer Wert
ec2:RekeyMarginTimeSeconds	Filtert den Zugriff nach Margenzeit bis zum Ablauf der Phase-2-Lebensdauer für einen VPN-Tunnel	Numerischer Wert
ec2:Remove/group	Filtert den Zugriff nach der Gruppe, die aus einem Snapshot entfernt wird	String
ec2:Remove/userId	Filtert den Zugriff nach der Konto-ID, die aus einem Snapshot entfernt wird	String

Bedingungsschlüssel	Beschreibung	Typ
ec2:ReplayWindowSizePackets	Filtert den Zugriff nach der Anzahl der Pakete in einem IKE-Wiedergabefenster	String
ec2:RequesterVpc	Filtert den Zugriff nach ARN einer Anforderer-VPC in einer VPC-Peering-Verbindung	ARN
ec2:ReservedInstancesOfferingType	Filtert den Zugriff nach Zahlungsoption des Reserved Instance-Angebots („No Upfront (Keine Vorauszahlung)“, „Partial Upfront (Teileweise Vorauszahlung)“ oder „All Upfront (Komplette Vorauszahlung)“)	String
ec2:ResourceTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paar einer Ressource	Zeichenfolge
ec2:RoleDelivery	Filtert den Zugriff nach Version des Instance-Metadaten-Service zum Abrufen von IAM-Rollen-Anmeldeinformationen für EC2	Numerischer Wert
ec2:RootDeviceType	Filtert den Zugriff nach Stammgerätetyp der Instance (ebs oder instance-store)	String
ec2:RouteTableID	Filtert den Zugriff nach der ID einer Routing-Tabelle	String
ec2:RoutingType	Filtert den Zugriff nach Routing-Typ für die VPN-Verbindung	Zeichenfolge
ec2:SamlProviderArn	Filtert den Zugriff nach dem ARN des IAM-SAML-Identitätsanbieters	ARN
ec2:SecurityGroupID	Filtert den Zugriff nach der ID einer Sicherheitsgruppe	String

Bedingungsschlüssel	Beschreibung	Typ
ec2:ServerCertificateArn	Filtert den Zugriff nach dem ARN des Serverzertifikats	ARN
ec2:SnapshotCoolOffPeriod	Filtert den Zugriff nach der Abkühlungsperiode des Konformitätsmodus	Numerischer Wert
ec2:SnapshotID	Filtert den Zugriff nach der ID eines Snapshots	String
ec2:SnapshotLockDuration	Filtert den Zugriff anhand der Dauer der Snapshot-Sperre	Numerischer Wert
ec2:SnapshotTime	Filtert den Zugriff nach der Initiierungszeit eines Snapshots	Zeichenfolge
ec2:SourceInstanceARN	Filtert den Zugriff nach ARN der Instance, von der die Anforderung stammt	ARN
ec2:SourceOutpostArn	Filtert den Zugriff nach ARN des Outposts, von dem die Anforderung stammt	ARN
ec2:Subnet	Filtert den Zugriff nach ARN des Subnetzes	ARN
ec2:SubnetID	Filtert den Zugriff nach der ID eines Subnetzes	String
ec2:Tenancy	Filtert den Zugriff nach der Tenancy der VPC oder Instance (Standard, dedizierter oder Host)	String
ec2:VolumeID	Filtert den Zugriff nach der ID eines Volumes	String
ec2:VolumeIops	Filtert den Zugriff nach der Anzahl der für das Volume bereitgestellten Ein-/Ausgabevorgänge pro Sekunde (IOPS)	Numerischer Wert
ec2:VolumeSize	Filtert den Zugriff nach der Größe des Volumes (in GiB)	Numerischer Wert

Bedingungsschlüssel	Beschreibung	Typ
ec2:VolumeThroughput	Filtert den Zugriff nach dem Durchsatz des Volumes, in MiBps	Numerischer Wert
ec2:VolumeType	Filtert den Zugriff nach dem Typ des Volumes (gp2, gp3, io1, io2, st1, sc1 oder Standard)	Zeichenfolge
ec2:Vpc	Filtert den Zugriff nach ARN der VPC	ARN
ec2:VpcID	Filtert den Zugriff nach der ID einer Virtual Private Cloud (VPC)	String
ec2:VpcPeeringConnectionID	Filtert den Zugriff nach der ID einer VPC-Peering-Verbindung	String
ec2:VpceServiceName	Filtert den Zugriff nach Name des VPC-Endpunktservice	String
ec2:VpceServiceOwner	Filtert den Zugriff durch den Service-Besitzer des VPC-Endpunktdienstes (Amazon, aws-marketplace oder eine ID) AWS-Konto	String
ec2:VpceServicePrivateDnsName	Filtert den Zugriff nach dem privaten DNS-Namen des VPC-Endpunktservice	String
ec2:transitGatewayAttachmentId	Filtert den Zugriff nach der ID eines Transit-Gateway-Anhangs	String
ec2:transitGatewayConnectPeerId	Filtert den Zugriff nach der ID eines Transit-Gateway-Connect-Peers	String
ec2:transitGatewayId	Filtert den Zugriff nach der ID eines Transit-Gateways	String

Bedingungsschlüssel	Beschreibung	Typ
ec2:transitGatewayMulticastDomainId	Filtert den Zugriff nach der ID einer Transit-Gateway-Multicast-Domäne	String
ec2:transitGatewayPolicyTableId	Filtert den Zugriff anhand der ID einer Richtlinientabelle für ein Transit-Gateway	String
ec2:transitGatewayRouteTableAnnouncementId	Filtert den Zugriff nach der ID einer Transit-Gateway-Routentabelle (Ankündigung)	String
ec2:transitGatewayRouteTableId	Filtert den Zugriff nach der ID einer Transit-Gateway-Routentabelle	String

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling (Servicepräfix: `autoscaling`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon EC2 Auto Scaling definierte Aktionen
- Von Amazon EC2 Auto Scaling definierte Ressourcentypen
- Bedingungsschlüssel für Amazon EC2 Auto Scaling

Von Amazon EC2 Auto Scaling definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AttachInstances	Gewährt die Berechtigung zum Hinzufügen einzelner oder mehrerer EC2-Instances an die angegebene Auto-Scaling-Gruppe	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
AttachLoadBalancerTargetGroups	Gewährt die Berechtigung zum Hinzufügen einzelner oder mehrerer Zielgruppen zu der angegebenen Auto-Scaling-Gruppe	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TargetGroupARNs	
AttachLoadBalancers	Gewährt die Berechtigung zum Hinzufügen einzelner oder mehrerer Lastenverteilungen an die angegebene Auto-Scaling-Gruppe	Schreiben	autoScalingGroup*	autoscaling:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
				autoscaling:LoadBalancerNames	
AttachTrafficSources	Gewährt die Berechtigung zum Anfügen einzelner oder mehrerer Dateiverkehrsquellen an eine Auto-Scaling-Gruppe	Schreiben	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TrafficSourceIdentifiers	
BatchDeleteScheduledAction	Gewährt die Berechtigung zum Löschen der angegebenen geplanten Aktionen	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchPutScheduledUpdateGroupAction	Gewährt die Berechtigung zur Erstellung oder Aktualisierung mehrerer geplanter Skalierungsaktionen für eine Auto-Scaling-Gruppe.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
CancelInstanceRefresh	Gewährt die Berechtigung zum Abbrechen einer laufenden Instance-AktualisierungsProduktion.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
CompleteLifecycleAction	Gewährt Berechtigungen für das Ausführen der Lebenszyklusaktion für das angegebene Token oder die angegebene Instance mit dem angegebenen Resultat	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAutoScalingGroup	Gewährt die Berechtigung zur Erstellung einer Auto-Scaling-Gruppe mit dem angegebenen Namen und den angegebenen Attributen	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	iam:CreateServiceLinkedRole iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				autoscaling:InstanceTypes autoscaling:LaunchConfigurationName autoscaling:LaunchTemplateVersionSpecified autoscaling:LoadBalancerNames autoscaling:MaxSize autoscaling:MinSize autoscaling:TargetGroupARNs autoscaling:Traffi	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				cSourceIdentifiers autoscaling:VPCZoneIdentifiers aws:RequestTag/${TagKey} aws:TagKeys	
CreateLaunchConfiguration	Gewährt die Berechtigung zum Erstellen einer Startkonfiguration.	Write	launchConfiguration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				autoscaling:ImageId autoscaling:InstanceType autoscaling:SpotPrice autoscaling:MetadataHttpTokens autoscaling:MetadataHttpPutResponseHopLimit autoscaling:MetadataHttpEndpoint	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateOrUpdateTags	Gewährt die Berechtigung zum Erstellen oder Aktualisieren des Tags, der mit der angegebenen Auto-Scaling-Gruppe verknüpft ist	Markieren	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAutoScalingGroup	Gewährt die Berechtigung zum Löschen der angegebenen Auto-Scaling-Gruppe	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteLaunchConfiguration	Gewährt die Berechtigung zum Löschen der angegebenen Startkonfiguration	Write	launchConfiguration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteLifecycleHook	Gewährt die Berechtigung zum Löschen des angegebenen Lebenszyklus-Hooks	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteNotificationConfiguration	Gewährt die Berechtigung zum Löschen der angegebenen Benachrichtigung	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeletePolicy	Gewährt die Berechtigung zum Löschen der angegebenen Auto-Scaling-Richtlinie	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteScheduledAction	Gewährt die Berechtigung zum Löschen der angegebenen geplanten Aktion	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteTags	Gewährt die Berechtigung zum Löschen des angegebenen Tags.	Markieren	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteWarmPool	Gewährt die Berechtigung zum Löschen des mit der Auto-Scaling-Gruppe verknüpften Warmpools	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DescribeAccountLimits	Gewährt die Berechtigung zum Beschreiben der aktuellen Auto-Scaling-Ressourcenlimits für Ihren AWS-Konto	List			
DescribeAdjustmentTypes	Gewährt die Berechtigung zur Beschreibung der Richtlinienanpassungstypen, die mit PutScalingPolicy verwendet werden können	List			
DescribeAutoScalingGroups	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Auto-Scaling-Gruppen. Wenn keine Liste mit Namen übergeben wird, beschreibt der Aufruf alle Auto-Scaling-Gruppen.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeAutoScalingInstances	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Auto-Scaling-Instances Wenn keine Liste übergeben wird, beschreibt der Aufruf alle Instances.	List			
DescribeAutoScalingNotificationTypes	Gewährt die Berechtigung zur Beschreibung der Benachrichtigungstypen, die von Auto Scaling unterstützt werden	List			
DescribeInstanceRefreshes	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Instance-Aktualisierungen für eine Auto Scaling-Gruppe	List			
DescribeLaunchConfigurations	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Startkonfigurationen Wenn Sie keine Liste mit Namen angeben, beschreibt der Aufruf alle Startkonfigurationen.	List			
DescribeLifecycleHookTypes	Gewährt die Berechtigung zur Beschreibung der verfügbaren Typen von Lebenszyklus-Hooks	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeLifecycleHooks	Gewährt die Berechtigung zur Beschreibung der Lebenszyklus-Hooks für die angegebene Auto-Scaling-Gruppe	List			
DescribeLoadBalancerTargetGroups	Gewährt die Berechtigung zur Beschreibung der Zielgruppen für die angegebene Auto-Scaling-Gruppe	List			
DescribeLoadBalancers	Gewährt die Berechtigung zur Beschreibung der Lebenszyklus-Hooks für die angegebene Auto-Scaling-Gruppe	List			
DescribeMetricCollectionTypes	Gewährt die Berechtigung zur Beschreibung der verfügbaren CloudWatch-Kennzahlen für Auto Scaling	List			
DescribeNotificationConfigurations	Gewährt die Berechtigung zur Beschreibung der Benachrichtigungsaktionen, die der angegebenen Auto-Scaling-Gruppe zugeordnet sind	List			
DescribePolicies	Gewährt die Berechtigung zur Beschreibung der Richtlinien für die angegebene Auto-Scaling-Gruppe	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeScalingActivities	Gewährt die Berechtigung zur Beschreibung einzelne oder mehrere Skalierungsaktivitäten für die angegebene Auto-Scaling-Gruppe	List			
DescribeScalingProcessTypes	Gewährt die Berechtigung für die Beschreibung der Scaling-Prozesstypen, die mit ResumeProcesses und SuspendProcesses verwendet werden können	List			
DescribeScheduledActions	Gewährt die Berechtigung zur Beschreibung der für die Auto-Scaling-Gruppe geplanten Aktionen, die nicht ausgeführt wurden	List			
DescribeTags	Gewährt die Berechtigung zum Beschreiben des angegebenen Tags.	Read			
DescribeTerminationPolicyTypes	Gewährt die Berechtigung zur Beschreibung der von Auto Scaling unterstützten Beendigungsrichtlinien	Auflisten			
DescribeTrafficSources	Gewährt die Berechtigung zur Beschreibung der Zielgruppen für die angegebene Auto-Scaling-Gruppe	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeWarmPool	Gewährt die Berechtigung zum Beschreiben des mit der Auto-Scaling-Gruppe verknüpften Warmpools	List			
DetachInstances	Gewährt die Berechtigung zur Entfernung einzelner oder mehrerer Instances aus der angegebenen Auto-Scaling-Gruppe	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DetachLoadBalancerTargetGroups	Gewährt die Berechtigung zur Trennung einzelner oder mehrerer Zielgruppen von der angegebenen Auto-Scaling-Gruppe	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TargetGroupARNs	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DetachLoadBalancers	Gewährt die Berechtigung zur Entfernung einzelner oder mehrerer Lastenverteilungen aus der angegebenen Auto-Scaling-Gruppe	Schreiben	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:LoadBalancerNames	
DetachTrafficSources	Gewährt die Berechtigung zum Trennen einzelner oder mehrerer Dateiverkehrsquellen von einer Auto-Scaling-Gruppe	Schreiben	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TrafficSourceIdentifiers	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisableMetricsCollection	Gewährt die Berechtigung zur Deaktivierung der Überwachung der angegebenen Kennzahlen für die angegebene Auto-Scaling-Gruppe	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
EnableMetricsCollection	Gewährt die Berechtigung zur Aktivierung der Überwachung der angegebenen Kennzahlen für die angegebene Auto-Scaling-Gruppe	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
EnterStandby	Gewährt die Berechtigung zur Verschiebung der angegebenen Instances in den Standby-Modus	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ExecutePolicy	Gewährt die Berechtigung, die angegebene Richtlinie auszuführen.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
ExitStandby	Gewährt die Berechtigung zur Verschiebung der angegebenen Instances aus dem Standby-Modus	Schreiben	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
GetPredictiveScalingForecast	Gewährt die Berechtigung zum Abrufen der Prognosedaten für eine prädiktive Skalierungsrichtlinie	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutLifecycleHook	Gewährt die Berechtigung zur Erstellung oder Aktualisierung eines Lebenszyklus-Hook für die angegebene Auto-Scaling-Gruppe	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
PutNotificationConfiguration	Gewährt die Berechtigung eine Auto-Scaling-Gruppe so zu konfigurieren, dass Benachrichtigungen gesendet werden, wenn die angegebenen Ereignisse auftreten	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
PutScalingPolicy	Gewährt die Berechtigung zum Erstellen oder Aktualisieren einer Richtlinie für eine Auto-Scaling-Gruppe	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutScheduledUpdateGroupAction	Gewährt die Berechtigung zur Erstellung oder Aktualisierung einer geplanten Skalierungsaktion für eine Auto-Scaling-Gruppe.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:MaxSize autoscaling:MinSize	
PutWarmPool	Gewährt die Berechtigung zum Erstellen oder Aktualisieren des Warmpools, der mit der angegebenen Auto-Scaling-Gruppe verknüpft ist	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RecordLifecycleActionHeartbeat	Gewährt die Berechtigung für die Aufzeichnung eines Heartbeats für die Lebenszyklusaktion, die dem angegebenen Token oder der angegebenen Instance zugeordnet ist	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
ResumeProcesses	Gewährt Berechtigungen zur Fortsetzung der angegebenen oder aller unterbrochenen Auto-Scaling-Prozesse für die angegebene Auto-Scaling-Gruppe	Schreiben	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
RollbackInstanceRefresh	Gewährt die Berechtigung zum Rollback einer laufenden Instance-AktualisierungsProduktion.	Schreiben	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SetDesiredCapacity	Gewährt die Berechtigung zum Festlegen der Größe der angegebenen Auto-Scaling-Gruppe	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
SetInstanceHealth	Gewährt die Berechtigung zum Festlegen des Status einer bestimmten Instance.	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
SetInstanceProtection	Gewährt die Berechtigung zum Aktualisieren der Instance-Schutzeinstellungen der angegebenen Instances	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartInstanceRefresh	Gewährt die Berechtigung zum Starten einer neuen Instance-AktualisierungsProduktion	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
SuspendProcesses	Gewährt die Berechtigung zur Unterbrechung der angegebenen oder aller Auto-Scaling-Prozesse für die angegebene Auto-Scaling-Gruppe	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
TerminateInstanceInAutoScalingGroup	Gewährt die Berechtigung zum Beenden der angegebenen Instance und der optionalen Anpassung der Gruppengröße	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateAutoScalingGroup	Gewährt die Berechtigung zur Konfiguration der angegebenen Auto-Scaling-Gruppe	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				autoscaling:InstanceTypes autoscaling:LaunchConfigurationName autoscaling:LaunchTemplateVersionSpecified autoscaling:MaxSize autoscaling:MinSize autoscaling:VPCZoneIdentifiers	

Von Amazon EC2 Auto Scaling definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden

können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
autoScalingGroup	`arn:${Partition}:autoscaling:${Region}:${Account}:autoScalingGroup:${GroupId}:autoScalingGroupName/${GroupFriendlyName}`	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}
launchConfiguration	`arn:${Partition}:autoscaling:${Region}:${Account}:launchConfiguration:${Id}:launchConfigurationName/${LaunchConfigurationName}`	

Bedingungsschlüssel für Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
autoscaling:ImageId	Filtert den Zugriff basierend auf der AMI-ID für die Startkonfiguration	Zeichenfolge
autoscaling:InstanceType	Filtert den Zugriff basierend auf dem Instance-Typ für die Startkonfiguration	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
autoscaling:InstanceTypes	Filtert den Zugriff basierend auf den Instance-Typen, die als Überschreibungen einer Startvorlage für eine Richtlinie für gemischte Instances vorhanden sind. Verwenden Sie dies, um zu ermitteln, welche Instance-Typen in der Richtlinie explizit definiert werden können.	Zeichenfolge
autoscaling:LaunchConfigurationName	Filtert den Zugriff basierend auf dem Namen einer Startkonfiguration	Zeichenfolge
autoscaling:LaunchTemplateVersionSpecified	Filtert den Zugriff danach, ob Benutzer eine beliebige Version einer Startvorlage oder nur die neueste oder die Standardversion angeben können	Bool
autoscaling:LoadBalancerNames	Filtert den Zugriff basierend auf dem Namen des Load Balancers	ArrayOfString
autoscaling:MaxSize	Filtert den Zugriff basierend auf der maximalen Skalierungsgröße in der Anforderung	Numerischer Wert
autoscaling:MetadataHttpEndpoint	Filtert den Zugriff basierend darauf, ob der HTTP-Endpunkt für den Instance-Metadaten-Service aktiviert ist	Zeichenfolge
autoscaling:MetadataHttpPutResponseHopLimit	Filtert den Zugriff nach zulässiger Anzahl von Hops beim Aufruf des Instance-Metadaten-Service	Numerischer Wert

Bedingungsschlüssel	Beschreibung	Typ
autoscaling:MetadataHttpTokens	Filtert den Zugriff danach, ob beim Aufruf des Instance-Metadaten-Service Token erforderlich sind (optional oder erforderlich)	Zeichenfolge
autoscaling:MinSize	Filtert den Zugriff basierend auf der minimalen Skalierungsgröße in der Anforderung	Numerischer Wert
autoscaling:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
autoscaling:SpotPrice	Filtert den Zugriff basierend auf dem Preis für Spot Instances für die Startkonfiguration	Numerischer Wert
autoscaling:TargetGroupARNs	Filtert den Zugriff basierend auf dem ARN einer Zielgruppe	ArrayOfARN
autoscaling:TrafficSourceIdentifiers	Filtert den Zugriff basierend auf dem Wert des Zugriffs	ArrayOfString
autoscaling:VPCZoneIdentifiers	Filtert den Zugriff basierend auf der ID einer VPC-Zone	ArrayOfString
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüsseln, die in der Anforderung übergeben werden.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2 Image Builder

Amazon EC2 Image Builder (Service-Präfix: `imagebuilder`) bietet die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontext-Schlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon EC2 Image Builder definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelImageCreation	Gewährt die Erlaubnis, eine Image-Erstellung abzubrechen	Schreiben	image*		
CancelLifecycleExecution	Gewährt die Berechtigung zum Abbrechen der Ausführung einer Lebenszyklusausführung	Schreiben	lifecycleExecution*		
CreateComponent	Gewährt die Berechtigung zum Erstellen einer neuen Komponente	Write	component*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateContainerRecipe	Gewährt die Berechtigung zum Erstellen eines neuen Container-Rezepts	Write	containerRecipe*	aws:RequestTag/${TagKey} aws:TagKeys	ecr:DescribeImages ecr:DescribeRepositories iam:CreateServiceLinkedRole imagebuilder:GetComponent imagebuilder:GetImage imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDistributionConfiguration	Gewährt die Berechtigung zum Erstellen einer neuen Distributionskonfiguration	Write	distributionConfiguration*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole imagebuilder:TagResource

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateImage	Gewährt die Berechtigung zum Erstellen eines neuen Images.	Write	image*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetInfrastructureConfiguration imagebuilder:GetWorkflow

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					imagebuilder:TagResource

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateImagePipeline	Gewährt die Berechtigung zum Erstellen einer neuen Image-Pipeline	Write	imagePipeline*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetInfrastructureConfiguration imagebuilder:GetWorkflow

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					imagebuilder:TagResource
CreateImageRecipe	Gewährt die Berechtigung zum Erstellen einers neuen Image-Rezepts	Write	imageRecipe*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeImages iam:CreateServiceLinkedRole imagebuilder:GetComponent imagebuilder:GetImage imagebuilder:TagResource

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateInfrastructureConfiguration	Gewährt die Berechtigung zum Erstellen einer neuen Infrastrukturkonfiguration	Schreiben	infrastructureConfiguration*	aws:RequestTag/${TagKey} aws:TagKeys imagebuilder:CreatedResourceTagKeys imagebuilder:CreatedResourceTag/<key> imagebuilder:Ec2MetadataHttpTokens imagebuilder:StatusTopicArn	iam:CreateServiceLinkedRole iam:PassRole imagebuilder:TagResource sns:Publish

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateLifecyclePolicy	Gewährt die Berechtigung zum Erstellen einer neuen Lebenszyklusrichtlinie	Schreiben	lifecyclePolicy*	aws:RequestTag/${TagKey} aws:TagKeys imagebuilder:LifecyclePolicyResourceType	iam:PassRole imagebuilder:TagResource
CreateWorkflow	Gewährt die Berechtigung zum Erstellen eines neuen Workflows	Schreiben	workflow*	aws:RequestTag/${TagKey} aws:TagKeys	imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext s3:GetObject s3:ListBucket

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteComponent	Gewährt die Berechtigung zum Löschen einer Komponente	Write	component*		
DeleteContainerRecipe	Gewährt die Berechtigung zum Löschen eines Container-Rezepts	Write	containerRecipe*		
DeleteDistributionConfiguration	Gewährt die Berechtigung zum Löschen der Distributionskonfiguration	Write	distributionConfiguration*		
DeleteImage	Gewährt die Berechtigung zum Löschen eines Images	Write	image*		
DeleteImagePipeline	Gewährt die Berechtigung zum Löschen einer Image-Pipeline	Write	imagePipeline*		
DeleteImageRecipe	Gewährt die Berechtigung zum Löschen eines Image-Rezepts	Write	imageRecipe*		
DeleteInfrastructureConfiguration	Gewährt die Berechtigung zum Löschen einer Infrastrukturkonfiguration	Schreiben	infrastructureConfiguration*		
DeleteLifecyclePolicy	Gewährt die Berechtigung zum Löschen einer Lebenszyklusrichtlinie	Schreiben	lifecyclePolicy*		
DeleteWorkflow	Gewährt die Berechtigung zum Löschen eines Workflows	Schreiben	workflow*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetComponent	Gewährt die Berechtigung zum Anzeigen von Details zu einer Komponente	Read	component*		kms:Decrypt
GetComponentPolicy	Gewährt die Berechtigung zum Anzeigen der mit einer Komponente verknüpften Ressourcenrichtlinie	Read	component*		
GetContainerRecipe	Gewährt die Berechtigung zum Anzeigen von Details zu einem Container-Rezept	Read	containerRecipe*		
GetContainerRecipePolicy	Gewährt die Berechtigung zum Anzeigen der einem Container-Rezept zugeordneten Ressourcenrichtlinie	Read	containerRecipe*		
GetDistributionConfiguration	Gewährt die Berechtigung zum Anzeigen von Details zu einer Distributionskonfiguration	Read	distributionConfiguration*		
GetImage	Gewährt die Berechtigung zum Anzeigen von Details zu einem Image	Read	image*	aws:ResourceTag/${TagKey}	
GetImagePipeline	Gewährt die Berechtigung zum Anzeigen von Details zu einer Image-Pipeline	Read	imagePipeline*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetImagePolicy	Gewährt die Berechtigung zum Anzeigen der mit einem Image verknüpften Ressourcenrichtlinie	Read	image*		
GetImageRecipe	Gewährt die Berechtigung zum Anzeigen von Details zu einem Image-Rezept	Read	imageRecipe*		
GetImageRecipePolicy	Gewährt die Berechtigung zum Anzeigen der mit einem Image-Rezept verknüpften Ressourcenrichtlinie	Read	imageRecipe*		
GetInfrastructureConfiguration	Gewährt die Berechtigung zum Anzeigen der Details zu einer Infrastrukturkonfiguration	Lesen	infrastructureConfiguration*		
GetLifecycleExecution	Gewährt die Berechtigung zum Anzeigen von Details zu einer Lebenszyklusausführung	Lesen	lifecycleExecution*		
GetLifecyclePolicy	Gewährt die Berechtigung zum Anzeigen von Details zu einer Lebenszyklusausführung	Lesen	lifecyclePolicy*		
GetWorkflow	Gewährt die Berechtigung zum Anzeigen von Details zu einem Workflow	Lesen	workflow*		kms:Decrypt
GetWorkflowExecution	Gewährt die Berechtigung zum Anzeigen von Details zu einer Workflow-Ausführung	Lesen	workflowExecution*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetWorkflowStepExecution	Gewährt die Berechtigung zum Anzeigen von Details zur Ausführung eines Workflow-Schritts	Lesen	workflowStepExecution*		
ImportComponent	Gewährt die Berechtigung zum Importieren einer neuen Komponente	Schreiben	component*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext
ImportVmImage	Gewährt die Berechtigung zum Importieren eines Images	Schreiben	image*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeImportImageTasks iam:CreateServiceLinkedRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListComponentBuildVersions	Gewährt die Berechtigung zum Auflisten der Komponenten-Buildversionen in Ihrem Konto	List	componentVersion*		
ListComponents	Gewährt die Berechtigung zum Auflisten der Komponentenversionen, die Ihrem Konto gehören oder für Ihr Konto freigegeben sind	List			
ListContainerRecipes	Gewährt die Berechtigung zum Auflisten der Container-Rezepte, die Ihrem Konto gehören oder mit ihm geteilt werden	List			
ListDistributionConfigurations	Gewährt die Berechtigung zum Auflisten die Verteilungskonfigurationen in Ihrem Konto	List			
ListImageBuildVersions	Gewährt die Berechtigung zum Auflisten der Image-Build-Versionen in Ihrem Konto	Auflisten	imageVersion*		
ListImagePackages	Gewährt die Berechtigung zum Zurückgeben einer Liste von Paketen, die auf dem angegebenen Image installiert sind	Auflisten	image*	aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListImagePipelineImages	Gewährt die Berechtigung zum Zurückgeben einer Liste von Images, die von der angegebenen Pipeline erstellt wurden	Auflisten	imagePipeline*		
ListImagePipelines	Gewährt die Berechtigung zum Auflisten der Image-Pipelines in Ihrem Konto	List			
ListImageRecipes	Gewährt die Berechtigung zum Auflisten der Image-Rezepte, die Ihrem Konto gehören oder mit ihm geteilt werden	Auflisten			
ListImageScanFindingAggregations	Gewährt die Berechtigung zum Auflisten der Aggregationen zu den Ergebnissen des Image-Scans in Ihrem Konto	Auflisten	image		
			imagePipeline		
ListImageScanFindings	Gewährt die Berechtigung zum Auflisten der Ergebnisse des Image-Scans für die Images in Ihrem Konto	Auflisten	image		inspector2:ListFindings
			imagePipeline		
ListImages	Gewährt die Berechtigung zum Auflisten der Image-Versionen, die Ihrem Konto gehören oder für Ihr Konto freigegeben sind	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListInfrastructureConfigurations	Gewährt die Berechtigung zum Auflisten der Infrastrukturkonfigurationen in Ihrem Konto	Auflisten			
ListLifecycleExecutionResources	Gewährt die Berechtigung zum Auflisten von Ressourcen für die angegebene Lebenszyklusausführung	Auflisten	lifecycleExecution*		
ListLifecycleExecutions	Gewährt die Berechtigung zum Auflisten von Lebenszyklusausführungen für die angegebene Ressource	Auflisten	image		
			lifecyclePolicy		
ListLifecyclePolicies	Gewährt die Berechtigung zum Auflisten der Lebenszyklusrichtlinien in Ihrem Konto	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Markierungen für eine Image-Builder-Ressource	Lesen	component	aws:ResourceTag/${TagKey}	
			containerRecipe	aws:ResourceTag/${TagKey}	
			distributionConfiguration	aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			image	aws:ResourceTag/${TagKey}	
			imagePipeline	aws:ResourceTag/${TagKey}	
			imageRecipe	aws:ResourceTag/${TagKey}	
			infrastructureConfiguration	aws:ResourceTag/${TagKey}	
			lifecyclePolicy	aws:ResourceTag/${TagKey}	
			workflow	aws:ResourceTag/${TagKey}	
ListWaitingWorkflowSteps	Gewährt die Berechtigung zum Auflisten wartenden Workflow-Schritte für das Anruferkonto	Auflisten			
ListWorkflowBuildVersions	Gewährt die Berechtigung zum Auflisten der IWorkflow -Build-Versionen in Ihrem Konto	Auflisten	workflowVersion*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListWorkflowExecutions	Gewährt die Berechtigung zum Auflisten von Workflow-Ausführungen für das angegebene Image	Auflisten	image*		
ListWorkflowStepExecutions	Gewährt die Berechtigung zum Auflisten von Workflow-Schrittausführungen für den angegebenen Workflow	Auflisten	workflowExecution*		
ListWorkflows	Gewährt die Berechtigung zum Auflisten der Workflow-Versionen, die Ihrem Konto gehören oder für Ihr Konto freigegeben sind	Auflisten			
PutComponentPolicy	Gewährt die Berechtigung zum Festlegen der mit einer Komponente verknüpften Ressourcenrichtlinie	Berechtigungsverwaltung	component*		
PutContainerRecipePolicy	Gewährt die Berechtigung zum Festlegen der einem Container-Rezept zugeordneten Ressourcenrichtlinie	Berechtigungsverwaltung	containerRecipe*		
PutImagePolicy	Gewährt die Berechtigung zum Festlegen der mit einem Image verknüpften Ressourcenrichtlinie	Berechtigungsverwaltung	image*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutImageRecipePolicy	Gewährt die Berechtigung zum Festlegen der mit einem Image-Rezept verknüpften Ressourcenrichtlinie	Berechtigungsverwaltung	imageRecipe*		
SendWorkflowStepAction	Gewährt die Berechtigung zum Senden einer Aktion an einen Workflow-Schritt	Schreiben	image* workflowStepExecution*		
StartImagePipelineExecution	Gewährt die Berechtigung zum Erstellen eines neuen Images aus einer Pipeline	Schreiben	imagePipeline*		iam:CreateServiceLinkedRole imagebuilder:GetImagePipeline
StartResourceStateUpdate	Gewährt die Berechtigung zum Starten einer Statusaktualisierung für die angegebene Ressource	Schreiben	image*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Markieren einer Image-Builder-Ressource	Markieren	component	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			containerRecipe	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			distributionConfiguration	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			image	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			imagePipeline	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			imageRecipe	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			infrastructureConfiguration	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			lifecyclePolicy	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			workflow	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Image-Builder-Ressource	Markieren	component	aws:ResourceTag/${TagKey} aws:TagKeys	
			containerRecipe	aws:ResourceTag/${TagKey} aws:TagKeys	
			distributionConfiguration	aws:ResourceTag/${TagKey} aws:TagKeys	
			image	aws:ResourceTag/${TagKey} aws:TagKeys	
			imagePipeline	aws:ResourceTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			imageRecipe	aws:ResourceTag/${TagKey} aws:TagKeys	
			infrastructureConfiguration	aws:ResourceTag/${TagKey} aws:TagKeys	
			lifecyclePolicy	aws:ResourceTag/${TagKey} aws:TagKeys	
			workflow	aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateDistributionConfiguration	Gewährt die Berechtigung zum Aktualisieren einer vorhandenen Distributionskonfiguration	Write	distributionConfiguration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateImagePipeline	Gewährt die Berechtigung, eine bestehende Image-Pipeline zu aktualisieren	Write	imagePipeline*		iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetInfrastructureConfiguration imagebuilder:GetWorkflow

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateInfrastructureConfiguration	Gewährt die Berechtigung zum Aktualisieren einer bestehenden Infrastrukturkonfiguration	Schreiben	infrastructureConfiguration*	aws:ResourceTag/${TagKey} imagebuilder:CreatedResourceTagKeys imagebuilder:CreatedResourceTag/<key> imagebuilder:Ec2MetadataHttpTokens imagebuilder:StatusTopicArn	iam:PassRole sns:Publish
UpdateLifecyclePolicy	Gewährt die Berechtigung, eine vorhandene Lebenszyklusrichtlinie zu aktualisieren	Schreiben	lifecyclePolicy*	imagebuilder:LifecyclePolicyResourceType	iam:PassRole

Vom Amazon EC2 Image Builder definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
component	`arn:${Partition}:imagebuilder:${Region}:${Account}:component/${ComponentName}/${ComponentVersion}/${ComponentBuildVersion}`	aws:ResourceTag/${TagKey}
componentVersion	`arn:${Partition}:imagebuilder:${Region}:${Account}:component/${ComponentName}/${ComponentVersion}`	aws:ResourceTag/${TagKey}
distributionConfiguration	`arn:${Partition}:imagebuilder:${Region}:${Account}:distribution-configuration/${DistributionConfigurationName}`	aws:ResourceTag/${TagKey}
image	`arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}/${ImageBuildVersion}`	aws:ResourceTag/${TagKey}
imageVersion	`arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}`	aws:ResourceTag/${TagKey}
imageRecipe	`arn:${Partition}:imagebuilder:${Region}:${Account}:image-recipe/${ImageRecipeName}/${ImageRecipeVersion}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
containerRecipe	arn:${Partition}:imagebuilder:${Region}:${Account}:container-recipe/${ContainerRecipeName}/${ContainerRecipeVersion}	aws:ResourceTag/${TagKey}
imagePipeline	arn:${Partition}:imagebuilder:${Region}:${Account}:image-pipeline/${ImagePipelineName}	aws:ResourceTag/${TagKey}
infrastructureConfiguration	arn:${Partition}:imagebuilder:${Region}:${Account}:infrastructure-configuration/${ResourceId}	aws:ResourceTag/${TagKey}
kmsKey	arn:${Partition}:kms:${Region}:${Account}:key/${KeyId}	
lifecycleExecution	arn:${Partition}:imagebuilder:${Region}:${Account}:lifecycle-execution/${LifecycleExecutionId}	
lifecyclePolicy	arn:${Partition}:imagebuilder:${Region}:${Account}:lifecycle-policy/${LifecyclePolicyName}	aws:ResourceTag/${TagKey}
workflow	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow/${WorkflowType}/${WorkflowName}/${WorkflowVersion}/${WorkflowBuildVersion}	aws:ResourceTag/${TagKey}
workflowVersion	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow/${WorkflowType}/${WorkflowName}/${WorkflowVersion}	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
workflowExecution	`arn:${Partition}:imagebuilder:${Region}:${Account}:workflow-execution/${WorkflowExecutionId}`	
workflowStepExecution	`arn:${Partition}:imagebuilder:${Region}:${Account}:workflow-step-execution/${WorkflowStepExecutionId}`	

Bedingungsschlüssel für Amazon EC2 Image Builder

Amazon EC2 Image Builder definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	String
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString
imagebuilder:Creat	Filtert den Zugriff durch die Tag-Schlüssel-Wert-Paare, die mit der Ressource verknüpft sind, die von Image Builder erstellt wurde.	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
edResourceTag/<key>		
imagebuilder:CreatedResourceTagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString
imagebuilder:Ec2MetadataHttpTokens	Filtert den Zugriff nach der in der Anforderung angegebenen HTTP-Token-Anforderung der EC2-Instance-Metadaten	String
imagebuilder:LifecyclePolicyResourceType	Filtert den Zugriff nach dem Ressourcentyp der Lebenszyklusrichtlinie, der in der Anforderung angegeben ist	String
imagebuilder:StatusTopicArn	Filtert den Zugriff nach dem SNS Topic Arn in der Anfrage, für die Terminalstatusbenachrichtigungen veröffentlicht werden	ARN

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2 Instance Connect

Amazon EC2 Instance Connect (Service-Präfix: `ec2-instance-connect`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.

- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon EC2 Instance Connect definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
OpenTunnel	Gewährt die Berechtigung zum Herstellen einer SSH-Verbindung zu der EC2-Instance mithilfe von EC2-Instance-Connect-Endpunkt	Schreiben	instance-connect-endpoint*		
			instance-connect-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2-instance-connect:remotePort ec2-instance-connect:privat	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				elpAddress ec2-instance-connect:MaxTunnelDuration	
SendSSHPublicKey	Gewährt die Berechtigung, einen öffentlichen SSH-Schlüssel an die angegebene EC2-Instance zu übertragen, die für Standard-SSH verwendet werden soll	Schreiben	instance*		
				ec2:osuser	
SendSerialConsoleSSHPublicKey	Gewährt die Berechtigung, einen öffentlichen SSH-Schlüssel an die angegebene EC2-Instance zu übertragen, die für SSH der seriellen Konsole verwendet werden soll	Schreiben	instance*		

Von Amazon EC2 Instance Connect definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
instance	`arn:${Partition}:ec2:${Region}:${Account}:instance/${InstanceId}`	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}
instance-connect-endpoint	`arn:${Partition}:ec2:${Region}:${Account}:instance-connect-endpoint/${InstanceConnectEndpointId}`	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon EC2 Instance Connect

Amazon EC2 Instance Connect definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf Tags, die der Ressource zugeordnet sind	Zeichenfolge
ec2-instance-connect:maxTunnelDuration	Filtert den Zugriff nach der maximalen Sitzungsdauer, die der Instance zugeordnet ist	Numerischer Wert

Bedingungsschlüssel	Beschreibung	Typ
ec2-instance-connect:privateIpAddress	Filtert den Zugriff nach der privaten IP-Adresse, die der Instance zugeordnet ist	IPAddress
ec2-instance-connect:remotePort	Filtert den Zugriff nach der Portnummer, die der Instance zugeordnet ist	Numerischer Wert
ec2:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf Tags, die der Ressource zugeordnet sind	Zeichenfolge
ec2:osuser	Filtert den Zugriff durch Angabe des Standardbenutzernamens für das AMI, das Sie zum Starten Ihrer Instance verwendet haben.	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EKS Auth

Amazon EKS Auth (Servicepräfix: `eks-auth`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon EKS Auth definierte Aktionen
- Von Amazon EKS Auth definierte Ressourcentypen
- Bedingungsschlüssel für Amazon EKS Auth

Von Amazon EKS Auth definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssumeRoleForPodIdentity	Erteilt die Erlaubnis, ein Kubernetes-Dienstkontotoken gegen temporäre Anmeldeinformationen auszutauschen AWS	Lesen	cluster*		

Von Amazon EKS Auth definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
cluster	`arn:${Partition}:eks:${Region}:${Account}:cluster/${ClusterName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon EKS Auth

Amazon EKS Auth definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert den Zugriff anhand eines Tag-Schlüssel-Wert-Paares	String

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elastic Beanstalk

AWS Elastic Beanstalk (Dienstpräfix:`elasticbeanstalk`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Elastic Beanstalk definierte Aktionen
- Von AWS Elastic Beanstalk definierte Ressourcentypen
- Bedingungsschlüssel für AWS Elastic Beanstalk

Von AWS Elastic Beanstalk definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AbortEnvironmentUpdate	Gewährt die Berechtigung zum Abbrechen des laufenden Updates der Umgebungskonfiguration oder der	Schreiben	environment*	elasticbeanstalk:InApplication	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Bereitstellung der Anwendungsversion				
AddTags	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Elastic-Beanstalk-Ressource und zum Aktualisieren von Tag-Werten	Tagging	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		
				aws:RequestTag/${TagKey} aws:TagKeys	
ApplyEnvironmentManagedAction	Gewährt die Berechtigung, eine geplante verwaltete Aktion sofort anzuwenden	Schreiben	environment*	elasticbeanstalk:InApplication	
AssociateEnvironmentOperationsRole	Gewährt die Berechtigung, eine Betriebsrolle mit einer Umgebung zu verknüpfen	Schreiben	environment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CheckDNSAvailability	Gewährt die Berechtigung zur Prüfung der CNAME-Verfügbarkeit	Lesen			
ComposeEnvironments	Gewährt die Berechtigung zum Erstellen oder Aktualisieren einer Gruppe von Umgebungen, die jeweils eine separate Komponente einer einzelnen Anwendung ausführen	Schreiben	application*		
			applicationversion*	elasticbeanstalk:InApplication	
CreateApplication	Gewährt die Berechtigung zum Erstellen einer neuen Anwendung	Schreiben	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateApplicationVersion	Gewährt die Berechtigung zum Erstellen einer Anwendungsversion für eine Anwendung	Schreiben	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			applicationversion*	elasticbeanstalk:InApplication aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfigurationTemplate	Gewährt die Berechtigung zum Erstellen einer Konfigurationsvorlage	Schreiben	configurationtemplate*	elasticbeanstalk:InApplication	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				elasticbeanstalk:FromApplication elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromEnvironment elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironment	Gewährt die Berechtigung zum Starten einer Umgebung für eine Anwendung	Schreiben	environment*	elasticbeanstalk:InApplication	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform aws:RequestTag/${TagKey} aws:TagKeys	
CreatePlatformVersion	Gewährt die Berechtigung zum Erstellen einer neuen Version einer benutzerdefinierten Plattform	Schreiben	platform*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStorageLocation	Gewährt die Berechtigung zum Erstellen des Amazon-S3-Speicherorts für das Konto	Schreiben			
DeleteApplication	Gewährt die Berechtigung zum Löschen einer Anwendung inklusive aller zugehörigen Versionen und Konfigurationen	Schreiben	application*		
DeleteApplicationVersion	Gewährt die Berechtigung zum Löschen einer Anwendungsversion aus einer Anwendung	Schreiben	applicationversion*	elasticbeanstalk:InApplication	
DeleteConfigurationTemplate	Gewährt die Berechtigung zum Löschen einer Konfigurationsvorlage	Schreiben	configurationtemplate*	elasticbeanstalk:InApplication	
DeleteEnvironmentConfiguration	Gewährt die Berechtigung zum Löschen des Konfigurationsentwurfs, der mit der ausgeführten Umgebung verknüpft ist	Schreiben	environment*	elasticbeanstalk:InApplication	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeletePlatformVersion	Gewährt die Berechtigung zum Löschen einer Version einer benutzerdefinierten Plattform	Schreiben	platform*		
DescribeAccountAttributes	Gewährt die Berechtigung zum Abrufen einer Liste von Kontoattributen, einschließlich Ressourcenkontingenten	Lesen			
DescribeApplicationVersions	Erteilt die Berechtigung zum Abrufen einer Liste von Anwendungsversionen, die in einem AWS Elastic Beanstalk Beanstalk-Speicher-Bucket gespeichert sind	Auflisten	applicationversion	elasticbeanstalk:InApplication	
DescribeApplications	Gewährt die Berechtigung zum Abrufen der Beschreibungen von vorhandenen Anwendungen	Auflisten	application		
DescribeConfigurationOptions	Gewährt die Berechtigung zum Abrufen von Beschreibungen von Umgebungskonfigurationsoptionen	Lesen	configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			solutionstack		
DescribeConfigurationSettings	Gewährt die Berechtigung zum Abrufen einer Beschreibung der Einstellungen für einen Konfigurationssatz	Lesen	configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	
DescribeEnvironmentHealth	Gewährt die Berechtigung zum Abrufen von Informationen über den allgemeinen Zustand einer Umgebung	Lesen	environment		
DescribeEnvironmentManagedActionHistory	Gewährt die Berechtigung zum Abrufen einer Liste der abgeschlossenen und fehlgeschlagenen verwalteten Aktionen einer Umgebung	Lesen	environment	elasticbeanstalk:InApplication	
DescribeEnvironmentManagedActions	Gewährt die Berechtigung zum Abrufen einer Liste der anstehenden und laufenden verwalteten Aktionen einer Umgebung	Lesen	environment	elasticbeanstalk:InApplication	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeEnvironmentResources	Erteilt die Berechtigung zum Abrufen einer Liste von AWS Ressourcen für eine Umgebung	Lesen	environment	elasticbeanstalk:InApplication	
DescribeEnvironments	Gewährt die Berechtigung zum Abrufen von Beschreibungen für vorhandene Umgebungen	Auflisten	environment	elasticbeanstalk:InApplication	
DescribeEvents	Gewährt die Berechtigung zum Abrufen einer Liste von Ereignisbeschreibungen, die einer Reihe von Kriterien entsprechen	Lesen	application		
			applicationversion	elasticbeanstalk:InApplication	
			configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	
DescribeInstancesHealth	Gewährt die Berechtigung zum Abrufen von ausführlichen Informationen über den Zustand der Umgebungs-Instances	Lesen	environment		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribePlatformVersion	Gewährt die Berechtigung zum Abrufen einer Beschreibung einer verwalteten Plattformversion	Lesen	platform		
DisassociateEnvironmentOperationsRole	Gewährt die Berechtigung zum Aufheben der Zuordnung einer Betriebsrolle zu einer Umgebung	Schreiben	environment*		
ListAvailableSolutionStacks	Gewährt die Berechtigung zum Abrufen einer Liste der verfügbaren Lösungsstack-Namen	Auflisten	solutionstack		
ListPlatformBranches	Gewährt die Berechtigung zum Abrufen einer Liste der verfügbaren Plattformzweige	Auflisten			
ListPlatformVersions	Gewährt die Berechtigung zum Abrufen einer Liste der verfügbaren Plattformen	Auflisten	platform		
ListTagsForResource	Gewährt die Berechtigung zum Abrufen einer Liste der Tags einer Elastic-Beanstalk-Ressource	Lesen	application		
			applicationversion		
			configurationtemplate		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			environment		
			platform		
PutInstanceStatistics	Gewährt die Berechtigung zum Übermitteln von Instance-Statistiken für einen verbesserten Zustand	Schreiben	application*		
			environment*		
RebuildEnvironment	Erteilt die Berechtigung, alle AWS Ressourcen für eine Umgebung zu löschen und neu zu erstellen und einen Neustart zu erzwingen	Schreiben	environment*	elasticbeanstalk:InApplication	
RemoveTags	Gewährt die Berechtigung zum Entfernen von Tags aus einer Elastic-Beanstalk-Ressource	Tagging	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RequestEnvironmentInfo	Gewährt die Berechtigung zum Initiieren einer Anforderung zum Kompilieren von Informationen über die bereitgestellte Umgebung	Lesen	environment*	elasticbeanstalk:InApplication	
RestartAppServer	Gewährt die Berechtigung, die Umgebung zu veranlassen, den Anwendungscontainer-Server neu zu starten, der auf jeder Amazon-EC2-Instance ausgeführt wird	Schreiben	environment*	elasticbeanstalk:InApplication	
RetrieveEnvironmentInfo	Erteilt die Erlaubnis, die kompilierten Informationen aus einer RequestEnvironmentInfo Anfrage abzurufen	Lesen	environment*	elasticbeanstalk:InApplication	
SwapEnvironmentCNAMEs	Gewährt die Berechtigung, die CNAMEs von zwei Umgebungen auszutauschen	Schreiben	environment*	elasticbeanstalk:InApplication	
				elasticbeanstalk:FromEnvironment	
TerminateEnvironment	Gewährt die Berechtigung zum Beenden einer Umgebung	Schreiben	environment*	elasticbeanstalk:InApplication	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateApplication	Gewährt die Berechtigung zum Aktualisieren einer Anwendung mit bestimmten Eigenschaften	Schreiben	application*		
UpdateApplicationResourceLifecycle	Gewährt die Berechtigung zum Aktualisieren der Lebenszyklusrichtlinie für die Anwendungsversion, die mit der Anwendung verknüpft ist	Schreiben	application*		
UpdateApplicationVersion	Gewährt die Berechtigung zum Aktualisieren einer Anwendungsversion mit bestimmten Eigenschaften	Schreiben	applicationversion*	elasticbeanstalk:InApplication	
UpdateConfigurationTemplate	Gewährt die Berechtigung zum Aktualisieren einer Konfigurationsvorlage mit bestimmten Eigenschaften oder Konfigurationsoptionswerten	Schreiben	configurationtemplate*	elasticbeanstalk:InApplication	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				elasticbeanstalk:FromApplication elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromEnvironment elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateEnvironment	Gewährt die Berechtigung zum Aktualisieren einer Umgebung.	Schreiben	environment*	elasticbeanstalk:InApplication	
				elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform	
UpdateTagsForResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Elastic-Beanstalk-Ressource, zum Entfernen von Tags und zum Aktualisieren von Tag-Werten	Tagging	application		
			applicationversion		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			configurationtemplate		
			environment		
			platform		
				aws:RequestTag/${TagKey} aws:TagKeys	
ValidateConfigurationSettings	Gewährt die Berechtigung, die Gültigkeit eines Satzes von Konfigurationseinstellungen für eine Konfigurationsvorlage oder eine Umgebung zu überprüfen	Lesen	configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	

Von AWS Elastic Beanstalk definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
application	`arn:${Partition}:elasticbeanstalk:${Region}:${Account}:application/${ApplicationName}`	aws:ResourceTag/${TagKey}
applicationversion	`arn:${Partition}:elasticbeanstalk:${Region}:${Account}:applicationversion/${ApplicationName}/${VersionLabel}`	aws:ResourceTag/${TagKey} elasticbeanstalk:InApplication
configurationtemplate	`arn:${Partition}:elasticbeanstalk:${Region}:${Account}:configurationtemplate/${ApplicationName}/${TemplateName}`	aws:ResourceTag/${TagKey} elasticbeanstalk:InApplication
environment	`arn:${Partition}:elasticbeanstalk:${Region}:${Account}:environment/${ApplicationName}/${EnvironmentName}`	aws:ResourceTag/${TagKey} elasticbeanstalk:InApplication
solutionstack	`arn:${Partition}:elasticbeanstalk:${Region}::solutionstack/${SolutionStackName}`	
platform	`arn:${Partition}:elasticbeanstalk:${Region}::platform/${PlatformNameWithVersion}`	

Bedingungsschlüssel für AWS Elastic Beanstalk

AWS Elastic Beanstalk definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung.	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf den Tag-Schlüssel-Wert-Paaren, die an die Ressource angefügt wurden.	Zeichenfolge
aws:TagKeys	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString
elasticbeanstalk:FromApplication	Filtert den Zugriff durch eine Anwendung als Abhängigkeit oder Einschränkung von einem Eingabeparameter	ARN
elasticbeanstalk:FromApplicationVersion	Filtert den Zugriff durch eine Anwendungsversion als Abhängigkeit oder Einschränkung von einem Eingabeparameter	ARN
elasticbeanstalk:FromConfigurationTemplate	Filtert den Zugriff durch eine Konfigurationsvorlage als Abhängigkeit oder Einschränkung von einem Eingabeparameter	ARN

Bedingungsschlüssel	Beschreibung	Typ
elasticbeanstalk:FromEnvironment	Filtert den Zugriff durch eine Umgebung als Abhängigkeit oder Beschränkung von einem Eingabeparameter	ARN
elasticbeanstalk:FromPlatform	Filtert den Zugriff durch eine Plattform als Abhängigkeit oder Beschränkung von einem Eingabeparameter	ARN
elasticbeanstalk:FromSolutionStack	Filtert den Zugriff eines Lösungs-Stacks als Abhängigkeit oder Beschränkung von einem Eingabeparameter	ARN
elasticbeanstalk:InApplication	Filtert den Zugriff durch eine Anwendung, die die Ressource enthält, für die die Aktion ausgeführt wird	ARN

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Elastic Block Store

Amazon Elastic Block Store (Servicepräfix: `ebs`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Elastic Block Store definierte Aktionen
- Von Amazon Elastic Block Store definierte Ressourcentypen

- Bedingungsschlüssel für Amazon Elastic Block Store

Von Amazon Elastic Block Store definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CompleteSnapshot	Gewährt die Berechtigung, den Snapshot zu versiegeln und zu vervollständigen, nachdem alle erforderlichen Datenblöcke in ihn geschrieben wurden	Schreiben	snapshot*		
				aws:ResourceTag/${TagKey}	
GetSnapshotBlock	Gewährt die Berechtigung zur Rückgabe der Daten eines Blocks in einem Amazon Elastic Block Store (EBS) Snapshot	Read	snapshot*		
				aws:ResourceTag/${TagKey}	
ListChangedBlocks	Gewährt die Berechtigung, die Blöcke aufzulisten, die sich zwischen zwei Amazon Elastic Block Store (EBS)-Snapshots desselben Volumes/Snapshot-Linie unterscheiden	Lesen	snapshot*		
				aws:ResourceTag/${TagKey}	
ListSnapshotBlocks	Gewährt die Berechtigung zum Auflisten der Blöcke in einem Amazon Elastic Block Store (EBS) -Snapshot	Lesen	snapshot*		
				aws:ResourceTag/${TagKey}	
PutSnapshotBlock	Gewährt die Berechtigung, einen Datenblock in einen Snapshot zu schreiben, der durch den StartSnapshot-Vorgang erstellt wurde	Schreiben	snapshot*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartSnapshot	Gewährt die Berechtigung zum Erstellen eines neuen EBS-Snapshots	Schreiben	snapshot		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ebs:Description ebs:ParentSnapshot ebs:VolumeSize	

Von Amazon Elastic Block Store definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
snapshot	`arn:${Partition}:ec2:${Region}::snapshot/${SnapshotId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ebs:Description ebs:ParentSnapshot ebs:VolumeSize

Bedingungsschlüssel für Amazon Elastic Block Store

Amazon Elastic Block Store definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wertepaaren, die in der Anforderung zulässig sind	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paar einer Ressource	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert den Zugriff nach Liste von Tag-Schlüsseln, die in der Anforderung zulässig sind	ArrayOfString
ebs:Description	Filtert den Zugriff durch die Beschreibung des zu erstellen den Snapshots	Zeichenfolge
ebs:ParentSnapshot	Filtert den Zugriff nach ID des übergeordneten Snapshots	Zeichenfolge
ebs:VolumeSize	Filtert den Zugriff nach der Größe des Volumes für den zu erstellenden Snapshot in GiB	Numerischer Wert

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Elastic Container Registry

Amazon Elastic Container Registry (Service-Präfix: `ecr`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Elastic Container Registry definierte Aktionen
- Von Amazon Elastic Container Registry definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Elastic Container Registry

Von Amazon Elastic Container Registry definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchCheckLayerAvailability	Gewährt die Berechtigung zum Überprüfen der Verfügbarkeit mehrerer Image-Ebenen in der angegebenen Registry und im angegebenen Repository	Read	repository*		
BatchDeleteImage	Gewährt die Berechtigung zum Löschen einer Liste angegebener Images in einem angegebenen Repository	Write	repository*		
BatchGetImage	Gewährt die Berechtigung zum Abrufen detaillierter Informationen für bestimmte Images in einem angegebenen Repository	Lesen	repository*		
BatchGetRepositoryScanningConfiguration	Gewährt die Berechtigung zum Abrufen der Repository-Scan-Konfiguration für eine Liste von Repositorys	Lesen	repository*		
BatchImportUpstreamImage [nur Berechtigung]	Gewährt die Berechtigung, das Image der Upstream-Registry abzurufen und in Ihre private Registry zu importieren	Schreiben			
CompleteLayerUpload	Gewährt die Berechtigung, Amazon ECR mitzuteilen, dass der Upload der Image-Ebene für die angegebene Registry, den angegeben	Schreiben	repository*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	en Repository-Namen und die angegebene Upload-ID abgeschlossen ist				
CreatePullThroughCacheRule	Gewährt die Berechtigung zum Erstellen einer neuen Pull-Through-Cache-Regel	Schreiben			iam:CreateServiceLinkedRole
CreateRepository	Gewährt die Berechtigung zum Erstellen eines Image-Repositorys	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	ecr:TagResource
CreateRepositoryCreationTemplate	Gewährt die Berechtigung zum Erstellen der Repository-Erstellungs-Vorlage	Schreiben			ecr:PutLifecyclePolicy ecr:SetRepositoryPolicy
DeleteLifecyclePolicy	Gewährt die Berechtigung zum Löschen der angegebenen Lebenszyklusrichtlinie	Schreiben	repository*		
DeletePullThroughCacheRule	Gewährt die Berechtigung zum Löschen der Pull-Through-Cache-Regel	Schreiben			
DeleteRegistryPolicy	Gewährt die Berechtigung zum Löschen der Registrierungsrichtlinie	Berechtigungsverwaltung			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteRepository	Gewährt die Berechtigung zum Löschen eines vorhandenen Image-Repositorys	Schreiben	repository*		
DeleteRepositoryCreationTemplate	Gewährt die Berechtigung zum Löschen der Repository-Erstellungs-Vorlage	Schreiben			
DeleteRepositoryPolicy	Gewährt die Berechtigung zum Löschen der Repository-Richtlinie aus einem angegebenen Repository	Berechtigungsverwaltung	repository*		
DescribeImageReplicationStatus	Gewährt die Berechtigung zum Abrufen des Replikationsstatus zu einem Image in einer Registry, einschließlich der Fehlerursache, wenn die Replikation fehlschlägt	Lesen	repository*		
DescribeImageScanFindings	Gewährt die Berechtigung zum Beschreiben der Ergebnisse des Image-Scans für das angegebene Image	Read	repository*		
DescribeImages	Gewährt die Berechtigung zum Abrufen von Metadaten zu den Images in einem Repository, einschließlich Image-Größe, Image-Tags und Erstellungsdatum	Auflisten	repository*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribePullThroughCacheRules	Gewährt die Berechtigung zum Beschreiben der Pull-Through-Cache-Regeln	Auflisten			
DescribeRegistry	Gewährt die Berechtigung zum Beschreiben der Registrierungseinstellungen	Read			
DescribeRepositories	Gewährt die Berechtigung zum Beschreiben von Image-Repositorys in einer Registry	Lesen	repository		
DescribeRepositoryCreationTemplate	Gewährt die Berechtigung zum Beschreiben der Repository-Erstellungs-Vorlage	Lesen			
GetAuthorizationToken	Gewährt die Berechtigung zum Abrufen eines Token, das für eine angegebene Registry 12 Stunden lang gültig ist	Read			
GetDownloadUrlForLayer	Gewährt die Berechtigung zum Abrufen der Download-URL, die einer Image-Ebene entspricht	Read	repository*		
GetLifecyclePolicy	Gewährt die Berechtigung zum Abrufen der angegebenen Lebenszyklusrichtlinie	Read	repository*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetLifecyclePolicyPreview	Gewährt die Berechtigung zum Abrufen der Ergebnisse der Vorschauanfrage zur angegebenen Lebenszyklusrichtlinie	Read	repository*		
GetRegistryPolicy	Gewährt die Berechtigung zum Abrufen der Registrierungsrichtlinie	Lesen			
GetRegistryScanningConfiguration	Gewährt die Berechtigung zum Abrufen der Konfiguration des Registry-Scans	Lesen			
GetRepositoryPolicy	Gewährt die Berechtigung zum Abrufen der Repository-Richtlinie für ein angegebenes Repository	Read	repository*		
InitiateLayerUpload	Gewährt die Berechtigung, Amazon ECR darüber zu informieren, dass Sie eine Image-Ebene hochladen möchten.	Write	repository*		
ListImages	Gewährt die Berechtigung zum Auflisten aller Image-IDs für ein bestimmtes Repository	List	repository*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für eine Amazon ECR-Ressource	Read	repository*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
PutImage	Gewährt die Berechtigung zum Erstellen oder Aktualisieren des Image-Manifests, das einem Image zugeordnet ist	Write	repository*		
PutImageScanningConfiguration	Gewährt die Berechtigung zum Aktualisieren der Image-Scan-Konfiguration für ein Repository	Write	repository*		
PutImageTagMutability	Gewährt die Berechtigung zum Aktualisieren der Einstellungen für die Veränderlichkeit der Image-Tags für ein Repository	Write	repository*		
PutLifecyclePolicy	Gewährt die Berechtigung zum Erstellen oder Aktualisieren einer Lebenszyklusrichtlinie	Write	repository*		
PutRegistryPolicy	Gewährt die Berechtigung zum Aktualisieren der Registrierungsrichtlinie	Berechtigungsverwaltung			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutRegistryScanningConfiguration	Gewährt die Berechtigung zum Aktualisieren der Konfiguration des Registry-Scans	Schreiben			
PutReplicationConfiguration	Gewährt die Berechtigung zum Aktualisieren der Replikationskonfiguration für die Registrierung	Schreiben			
ReplicateImage [nur Berechtigung]	Gewährt die Berechtigung zum Replizieren von Images in die Zielregistrierung	Write	repository*		
SetRepositoryPolicy	Gewährt die Berechtigung zum Anwenden einer Repository-Richtlinie auf ein angegebenes Repository, um die Zugriffsberechtigungen zu steuern	Berechtigungsverwaltung	repository*		
StartImageScan	Gewährt die Berechtigung zum Starten eines Image-Scans	Write	repository*		
StartLifecyclePolicyPreview	Gewährt die Berechtigung zum Starten einer Vorschau der angegebenen Lebenszyklusrichtlinie	Write	repository*		
TagResource	Gewährt die Berechtigung zum Markieren einer Amazon ECR-Ressource	Markieren	repository*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Amazon ECR-Ressource	Markierung	repository*		
				aws:TagKeys	
UpdatePullThroughCacheRule	Gewährt die Berechtigung zum Aktualisieren der Pull-Through-Cache-Regel	Schreiben			
UploadLayerPart	Gewährt die Berechtigung zum Upload eines Teils einer Image-Ebene in Amazon ECR	Schreiben	repository*		
ValidatePullThroughCacheRule	Gewährt die Berechtigung zum Validieren der Pull-Through-Cache-Regel	Lesen			

Von Amazon Elastic Container Registry definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
repository	`arn:${Partition}:ecr:${Region}:${Account}:repository/${RepositoryName}`	aws:ResourceTag/${TagKey} ecr:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Elastic Container Registry

Amazon Elastic Container Registry definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den zulässigen Werten für jeden der Tags	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Tag-Wert, der der Ressource zugeordnet ist	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach dem Vorhandensein verbindlicher Tags in der Anforderung	ArrayOfString
ecr:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Tag-Wert, der der Ressource zugeordnet ist	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Elastic Container Registry Public

Amazon Elastic Container Registry Public (Service-Präfix: `ecr-public`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Elastic Container Registry Public definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie

den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchCheckLayerAvailability	Gewährt die Berechtigung zum Überprüfen der Verfügbarkeit mehrerer Image-Ebenen in der angegebenen Registry und im angegebenen Repository	Read	repository*		
BatchDeleteImage	Gewährt die Berechtigung zum Löschen einer Liste angegebener Images in einem angegebenen Repository	Write	repository*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CompleteLayerUpload	Gewährt die Berechtigung, Amazon ECR mitzuteilen, dass der Upload der Image-Ebene für die angegebene Registry, den angegebenen Repository-Namen und die angegebene Upload-ID abgeschlossen ist	Write	repository*		
CreateRepository	Gewährt die Berechtigung zum Erstellen eines Image-Repositorys	Write	repository*		ecr-public:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteRepository	Gewährt die Berechtigung zum Löschen eines vorhandenen Image-Repositorys	Write	repository*		
DeleteRepositoryPolicy	Gewährt die Berechtigung zum Löschen der Repository-Richtlinie aus einem angegebenen Repository	Write	repository*		
DescribeImageTags	Gewährt die Berechtigung zum Beschreiben aller Image-Tags für ein bestimmtes Repository	List	repository*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeImages	Gewährt die Berechtigung zum Abrufen von Metadaten zu den Images in einem Repository, einschließlich Image-Größe, Image-Tags und Erstellungsdatum	Read	repository*		
DescribeRegistries	Gewährt die Berechtigung zum Abrufen der einer Registrierung zugeordneten Katalogdaten	List	registry*		
DescribeRepositories	Gewährt die Berechtigung zum Beschreiben von Image-Repositorys in einer Registry	List	repository		
GetAuthorizationToken	Gewährt die Berechtigung zum Abrufen eines Token, das für eine angegebene Registry 12 Stunden lang gültig ist	Read			
GetRegistryCatalogData	Gewährt die Berechtigung zum Abrufen der einer Registrierung zugeordneten Katalogdaten	Read	registry*		
GetRepositoryCatalogData	Gewährt die Berechtigung zum Abrufen der einem Repository zugeordneten Katalogdaten	Read	repository*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetRepositoryPolicy	Gewährt die Berechtigung zum Abrufen der Repository-Richtlinie für ein angegebenes Repository	Read	repository*		
InitiateLayerUpload	Gewährt die Berechtigung, Amazon ECR darüber zu informieren, dass Sie eine Image-Ebene hochladen möchten.	Write	repository*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für eine Amazon ECR-Ressource	Read	repository*		
PutImage	Gewährt die Berechtigung zum Erstellen oder Aktualisieren des Image-Manifests, das einem Image zugeordnet ist	Write	repository*		
PutRegistryCatalogData	Gewährt die Berechtigung zum Erstellen und Aktualisieren der einer Registrierung zugeordneten Katalogdaten	Write	registry*		
PutRepositoryCatalogData	Gewährt die Berechtigung zum Aktualisieren der einem Repository zugeordneten Katalogdaten	Write	repository*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SetRepositoryPolicy	Gewährt die Berechtigung zum Anwenden einer Repository-Richtlinie auf ein angegebenes Repository, um die Zugriffsberechtigungen zu steuern	Berechtigungsverwaltung	repository*		
TagResource	Gewährt die Berechtigung zum Markieren einer Amazon ECR-Ressource	Markieren	repository*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Amazon ECR-Ressource	Markieren	repository*		
				aws:TagKeys	
UploadLayerPart	Gewährt die Berechtigung zum Upload eines Teil einer Image-Ebene in Amazon ECR Public Teil einer Image-Ebene in Amazon ECR Public	Write	repository*		

Von Amazon Elastic Container Registry Public definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der

Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
repository	`arn:${Partition}:ecr-public::${Account}:repository/${RepositoryName}`	aws:ResourceTag/${TagKey} ecr-public:ResourceTag/${TagKey}
registry	`arn:${Partition}:ecr-public::${Account}:registry/${RegistryId}`	

Bedingungsschlüssel für Amazon Elastic Container Registry Public

Amazon Elastic Container Registry Public definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Anfragen zum Erstellen basierend auf den zulässigen Werten für jedes der Tags.	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf dem Tag-Wert, der der Ressource zugeordnet ist.	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert Anfragen zum Erstellen basierend auf dem Vorhandensein obligatorischer Tags in der Anfrage.	ArrayOfString
ecr-public:ResourceTag/${TagKey}	Filtert Aktionen basierend auf dem Tag-Wert, der der Ressource zugeordnet ist.	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für den Amazon Elastic Container Service

Amazon EC2 Container Service (Service-Präfix: `ecs`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Elastic Container Service definierte Aktionen
- Von Amazon Elastic Container Service definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Elastic Container Service

Von Amazon Elastic Container Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCapacityProvider	Gewährt die Berechtigung, einen neuen Kapazität sanbieter zu erstellen. Kapazitätsanbieter sind einem Amazon-ECS-Cluster zugeordnet und werden in Kapazitätsanbieterstrategien verwendet, um die das Auto Scaling des Clusters zu ermöglichen	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCluster	Gewährt die Berechtigung zum Erstellen eines neuen Amazon-ECS-Clusters	Write	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys ecs:capacity-provider	
CreateService	Gewährt die Berechtigung zum Ausführen und Verwalten einer gewünschten Anzahl von Aufgaben aus einer bestimmten Aufgabendefinition über die Service-Erstellung	Write	service*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys ecs:cluster ecs:capacity-provider ecs:task-definition ecs:enable-ebs-volumes ecs:enable-execute-command ecs:enable-service-connect ecs:namespace	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTaskSet	Gewährt die Berechtigung zum Erstellen eines neuen Amazon-ECS-Aufgabensatzes	Write		aws:RequestTag/${TagKey} aws:TagKeys ecs:cluster ecs:capacity-provider ecs:service ecs:task-definition	
DeleteAccountSetting	Gewährt die Berechtigung zum Ändern des ARN und des Formats der Ressourcen-ID einer Ressource für einen bestimmten IAM-Benutzer, eine IAM-Rolle oder den Stammbenutzer eines Kontos. Sie können festlegen, ob der neue ARN und das Format der Ressourcen-ID für die neu zu erstellenden Ressourcen deaktiviert werden sollen	Write		ecs:account-setting	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteAttributes	Gewährt die Berechtigung zum Löschen eines oder mehrerer benutzerdefinierter Attribute aus einer Amazon-ECS-Ressource	Write	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	
DeleteCapacityProvider	Gewährt die Berechtigung zum Löschen des angegebenen Kapazitätsanbieters	Write	capacity-provider*		
				aws:ResourceTag/${TagKey}	
DeleteCluster	Gewährt die Berechtigung zum Löschen des angegebenen Clusters	Write	cluster*		
				aws:ResourceTag/${TagKey}	
DeleteService	Gewährt die Berechtigung zum Löschen eines bestimmten Service innerhalb eines Clusters	Schreiben	service*		
				aws:ResourceTag/${TagKey} ecs:cluster	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteTaskDefinitions	Gewährt die Berechtigung zum Löschen der angegebenen Aufgabendefinitionen nach Familie und Revision	Schreiben	task-definition*		
				aws:ResourceTag/${TagKey}	
DeleteTaskSet	Gewährt die Berechtigung zum Löschen des angegebenen Aufgabensatzes	Write	task-set*		
				aws:ResourceTag/${TagKey} ecs:cluster ecs:service	
DeregisterContainerInstance	Gewährt die Berechtigung zum Abmelden einer Amazon-ECS-Container-Instance vom angegebenen Cluster	Write	cluster*		
				aws:ResourceTag/${TagKey}	
DeregisterTaskDefinition	Gewährt die Berechtigung zum Abmelden einer angegebenen Aufgabendefinition nach Familie und Revision	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeCapacityProviders	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer Amazon-ECS-Kapazitätsanbieter	Read	capacity-provider*		
				aws:ResourceTag/${TagKey}	
DescribeClusters	Gewährt die Berechtigung zum Beschreiben einer oder mehrerer Cluster	Read	cluster*		
				aws:ResourceTag/${TagKey}	
DescribeContainerInstances	Gewährt die Berechtigung zum Beschreiben von Amazon-ECS-Container-Instances	Read	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	
DescribeServices	Gewährt die Berechtigung zum Beschreiben der angegebenen Services, die in Ihrem Cluster ausgeführt werden	Read	service*		
				aws:ResourceTag/${TagKey} ecs:cluster	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeTaskDefinition	Gewährt die Berechtigung zum Beschreiben einer Aufgabendefinition. Sie können eine Familie und Revision angeben, um Informationen zu einer bestimmten Aufgabend efinition zu suchen, oder einfach die Familie angeben, um die neueste ACTIVE-Revision in dieser Familie zu ermitteln.	Read			
DescribeTaskSets	Gewährt die Berechtigung zum Beschreiben von Amazon-ECS-Aufgabensätzen	Read	task-set*		
				aws:ResourceTag/${TagKey} ecs:cluster ecs:service	
DescribeTasks	Gewährt die Berechtigung zum Beschreiben eines bestimmten Projekts.	Read	task*		
				aws:ResourceTag/${TagKey} ecs:cluster	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DiscoverPollEndpoint	Gewährt die Berechtigung einen Endpunkt für den Amazon-ECS-Agent zu erhalten, um Updates abzufragen	Write			
ExecuteCommand	Gewährt die Berechtigung, einen Befehl auf einem Amazon-ECS-Container remote auszuführen	Schreiben	cluster* task*	aws:ResourceTag/${TagKey} ecs:cluster ecs:container-name ecs:task	
GetTaskProtection	Gewährt die Berechtigung zum Abrufen des Schutzstatus von Aufgaben in einem Amazon ECS-Service	Lesen	task*	aws:ResourceTag/${TagKey} ecs:cluster	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAccountSettings	Gewährt die Berechtigung zum Auflisten der Kontoeinstellungen für eine Amazon-ECS-Ressource für einen bestimmten Prinzipal	Read			
ListAttributes	Gewährt die Berechtigung zum Auflisten der Attribute für Amazon-ECS-Ressourcen innerhalb eines bestimmten Zieltyps und Clusters	List	cluster*		
				aws:ResourceTag/${TagKey}	
ListClusters	Gewährt die Berechtigung zum Abrufen einer Liste bestehender Cluster	List			
ListContainerInstances	Gewährt die Berechtigung zum Abrufen einer Liste von Container-Instances in einem bestimmten Cluster	List	cluster*		
				aws:ResourceTag/${TagKey}	
ListServices	Gewährt die Berechtigung zum Abrufen einer Liste von Services, die in einem bestimmten Cluster ausgeführt werden	Auflisten		ecs:cluster	
ListServicesByNamespace	Erteilt die Berechtigung, eine Liste von Diensten abzurufen, die in einem bestimmten AWS Cloud Map-Namespace ausgeführt werden	Auflisten		ecs:namespace	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Abrufen von Tags für die angegebene Ressource	Read	capacity-provider		
			cluster		
			container-instance		
			service		
			task		
			task-definition		
			task-set		
				aws:ResourceTag/${TagKey}	
ListTaskDefinitionFamilies	Gewährt die Berechtigung zum Abrufen einer Liste von Aufgabendefinitionsfamilien, die bei Ihrem Konto registriert sind (dies kann Aufgabendefinitionsfamilien umfassen, die keine ACTIVE-Aufgabendefinitionen mehr enthalten)	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTaskDefinitions	Gewährt die Berechtigung zum Abrufen einer Liste der Aufgabendefinitionen, die bei Ihrem Konto registriert sind	List			
ListTasks	Gewährt die Berechtigung zum Abrufen einer Aufgabenliste für einen bestimmten Cluster	List	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	
Poll [nur Berechtigung]	Gewährt einem Agenten die Berechtigung, eine Verbindung zum Amazon ECS Service herzustellen, um den Status zu melden und Befehle abzurufen	Write	container-instance*		
				ecs:cluster	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutAccountSetting	Gewährt die Berechtigung zum Ändern des ARN und des Formats der Ressourcen-ID einer Ressource für einen bestimmten IAM-Benutzer, eine IAM-Rolle oder den Stammbenutzer eines Kontos. Sie können festlegen, ob der neue ARN und das Format der Ressourcen-ID für die neu zu erstellenden Ressourcen aktiviert werden sollen. Das Aktivieren dieser Einstellung ist erforderlich, um neue Amazon-ECS-Funktionen wie beispielsweise Ressourcen-Tagging zu verwenden	Write		ecs:account-setting	
PutAccountSettingDefault	Gewährt die Berechtigung zum Ändern des ARN und des Formats der Ressourcen-ID eines Ressourcentyps für alle IAM-Benutzer eines Kontos, für die keine einzelnen Kontoeinstellungen festgelegt wurden. Das Aktivieren dieser Einstellung ist erforderlich, um neue Amazon-ECS-Funktionen wie beispielsweise Ressourcen-Tagging zu verwenden	Write		ecs:account-setting	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutAttributes	Gewährt die Berechtigung zum Erstellen oder Aktualisieren eines Attributs auf einer Amazon-ECS-Ressource	Write	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	
PutClusterCapacityProviders	Gewährt die Berechtigung zum Ändern der verfügbaren Kapazitätsanbieter und der Standardstrategie des Kapazitätsanbieters für einen Cluster	Write	cluster*		
				aws:ResourceTag/${TagKey} ecs:capacity-provider	
RegisterContainerInstance	Gewährt die Berechtigung zum Registrieren einer EC2-Instance im angegebenen Cluster	Write	cluster*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RegisterTaskDefinition	Gewährt die Berechtigung zum Registrieren einer neuen Aufgabendefinition aus der übergebenen Familie und aus containerDefinitions	Write		aws:RequestTag/${TagKey} aws:TagKeys	
RunTask	Gewährt die Berechtigung zum Starten einer Aufgabe mit zufälliger Platzierung und dem Amazon-ECS-Standard-Scheduler.	Write	task-definition*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys ecs:cluster ecs:capacity-provider ecs:enable-ebs-volumes ecs:enable-execute-command	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartTask	Gewährt die Berechtigung zum Starten einer neuen Aufgabe aus der angegebenen Aufgabendefinition in der angegebenen Container-Instance oder den Instances	Write	task-definition*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys ecs:cluster ecs:container-instances ecs:enable-ebs-volumes ecs:enable-execute-command	
StartTelemetrySession	Gewährt die Berechtigung zum Starten einer Telemetriesitzung.	Write	container-instance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ecs:cluster	
StopTask	Gewährt die Berechtigung zum Beenden einer ausgeführten Aufgabe	Write	task*		
				aws:ResourceTag/${TagKey} ecs:cluster	
SubmitAttachmentStateChanges	Gewährt die Berechtigung zum Senden einer Bestätigung, dass Anhänge den Status geändert haben	Write	cluster*		
				aws:ResourceTag/${TagKey}	
SubmitContainerStateChange	Gewährt die Berechtigung zum Senden einer Bestätigung, dass ein Container den Status geändert hat	Write	cluster*		
				aws:ResourceTag/${TagKey}	
SubmitTaskStateChange	Gewährt die Berechtigung zum Senden einer Bestätigung, dass eine Aufgabe den Status geändert hat	Write	cluster*		
				aws:ResourceTag/${TagKey}	
TagResource	Gewährt die Berechtigung zum Markieren der angegebenen Ressource	Markieren	capacity-provider		
			cluster		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			container-instance		
			service		
			task		
			task-definition		
			task-set		
				aws:TagKeys aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} ecs:CreateAction	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung der angegebenen Ressource	Markieren	capacity-provider		
			cluster		
			container-instance		
			service		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			task		
			task-definition		
			task-set		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCapacityProvider	Gewährt die Berechtigung zum Aktualisieren des angegebenen Kapazitätsanbieters	Write	capacity-provider*		
				aws:ResourceTag/${TagKey}	
UpdateCluster	Gewährt die Berechtigung zum Ändern der Konfiguration oder der Einstellungen, die für einen Cluster verwendet werden sollen	Write	cluster*		
				aws:ResourceTag/${TagKey}	
UpdateClusterSettings	Gewährt die Berechtigung zum Ändern der Einstellungen, die für einen Cluster verwendet werden sollen	Write	cluster*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateContainerAgent	Gewährt die Berechtigung zum Aktualisieren der Amazon ECS-Container-Agenten auf einer angegebenen Container-Instance	Write	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	
UpdateContainerInstancesState	Gewährt die Berechtigung für den Benutzer zum Ändern des Status einer Amazon-ECS-Container-Instance	Write	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	
UpdateService	Gewährt die Berechtigung zum Ändern der Parameter eines Service	Write	service*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} ecs:cluster ecs:capacity-provider ecs:enable-ebs-volumes ecs:enable-execute-command ecs:enable-service-connect ecs:namespace ecs:task-definition	
UpdateServicePrimaryTaskSet	Gewährt die Berechtigung zum Ändern des primären in einem Service verwendeten Aufgabensatzes	Schreiben	service*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} ecs:cluster	
UpdateTaskProtection	Gewährt die Berechtigung zum Ändern des Schutzstatus einer Aufgabe	Schreiben	task*		
				aws:ResourceTag/${TagKey} ecs:cluster	
UpdateTaskSet	Gewährt die Berechtigung zum Aktualisieren des angegebenen Aufgabensatzes	Write	task-set*		
				aws:ResourceTag/${TagKey} ecs:cluster ecs:service	

Von Amazon Elastic Container Service definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
cluster	`arn:${Partition}:ecs:${Region}:${Account}:cluster/${ClusterName}`	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}
container-instance	`arn:${Partition}:ecs:${Region}:${Account}:container-instance/${ClusterName}/${ContainerInstanceId}`	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}
service	`arn:${Partition}:ecs:${Region}:${Account}:service/${ClusterName}/${ServiceName}`	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}
task	`arn:${Partition}:ecs:${Region}:${Account}:task/${ClusterName}/${TaskId}`	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}
task-definition	`arn:${Partition}:ecs:${Region}:${Account}:task-definition/${TaskDefinitionFamilyName}:${TaskDefinitionRevisionNumber}`	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}
capacity-provider	`arn:${Partition}:ecs:${Region}:${Account}:capacity-provider/${CapacityProviderName}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
		ecs:ResourceTag/${TagKey}
task-set	arn:${Partition}:ecs:${Region}:${Account}:task-set/${ClusterName}/${ServiceName}/${TaskSetId}	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Elastic Container Service

Amazon EC2 Container Service definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	String
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüsselwertpaaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString
ecs:CreateAction	Filtert den Zugriff nach Name einer ressourcenerstellenden API-Aktion	String

Bedingungsschlüssel	Beschreibung	Typ
ecs:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüsselwertpaaren, die der Ressource angefügt sind	String
ecs:account-setting	Filtert den Zugriff nach dem Amazon-ECS-Kontoeinstellungsnamen	String
ecs:capacity-provider	Filtert den Zugriff durch den ARN eines Amazon-ECS-Kapazitätsanbieters	ARN
ecs:cluster	Filtert den Zugriff anhand des ARNs eines Amazon ECS-Clusters	ARN
ecs:container-instances	Filtert den Zugriff durch den ARN eines Amazon ECS-Container-Instance	ARN
ecs:container-name	Filtert den Zugriff durch den Namen eines Amazon ECS-Containers, der in der ECS-Aufgabendefinition definiert ist	String
ecs:enable-ebs-volumes	Filtert den Zugriff nach der von Amazon ECS verwalteten Amazon EBS-Volume-Funktion Ihrer ECS-Aufgabe oder Ihres ECS-Service	String
ecs:enable-execute-command	Filtert den Zugriff durch die Execute-Command-Fähigkeit Ihrer Amazon ECS-Aufgabe oder des Amazon-ECS-Service	String
ecs:enable-service-connect	Filtert den Zugriff durch den Wert des Feldes in der Service-Connect-Konfiguration	String
ecs:namespace	Filtert den Zugriff nach dem ARN des AWS Cloud Map-Namespace, der in der Service Connect-Konfiguration definiert ist	ARN
ecs:service	Filtert den Zugriff durch den ARN eines Amazon-ECS-Service	ARN

Bedingungsschlüssel	Beschreibung	Typ
ecs:task	Filtert den Zugriff durch den ARN einer Amazon ECS-Aufgabe	ARN
ecs:task-definition	Filtert den Zugriff durch den ARN einer Amazon ECS-Aufgabendefinition	ARN

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elastic Disaster Recovery

AWS Elastic Disaster Recovery (Servicepräfix: `drs`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Elastic Disaster Recovery definierte Aktionen
- Von AWS Elastic Disaster Recovery definierte Ressourcentypen
- Bedingungsschlüssel für AWS Elastic Disaster Recovery

Von AWS Elastic Disaster Recovery definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateFailbackClientToRecoveryInstanceForDrs [nur Berechtigung]	Gewährt die Berechtigung, um den zugehörigen Failback-Client zur Wiederherstellungs-Instance abzurufen	Schreiben	RecoveryInstanceResource*		
AssociateSourceNetworkStack	Gewährt die Berechtigung zum Zuordnen vom CloudFormation-Stack an das Quellnetzwerk	Schreiben	SourceNetworkResource*		cloudformation:DescribeStackResource cloudformation:DescribeStacks drs:GetLaunchConfiguration ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplateVersions

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:ModifyLaunchTemplate
				aws:RequestTag/${TagKey} aws:TagKeys	
BatchCreateVolumeSnapshotGroupForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer Volume-Snapshot-Gruppe im Batch	Schreiben	RecoveryInstanceResource*		
			SourceServerResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchDeleteSnapshotRequestForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Löschen von Batches von Schnapshot-Anfragen	Schreiben			
CreateConvertedSnapshotForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines konvertierten Snapshots	Schreiben	SourceServerResource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExtendedSourceServer	Gewährt die Berechtigung zum Erweitern eines Quellservers	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	drs:DescribeSourceServers drs:GetReplicationConfiguration
CreateLaunchConfigurationTemplate	Gewährt die Berechtigung zum Erstellen einer Startkonfigurationsvorlage	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateRecoveryInstanceForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer Wiederherstellungs-Instance	Schreiben	SourceServerResource*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateReplicationConfigurationTemplate	Gewährt die Berechtigung zum Erstellen einer Replikationskonfigurationsvorlage	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetEbsDefaultKmsKeyId ec2:GetEbsEncryptionByDefault kms:CreateGrant kms:DescribeKey
CreateSourceNetwork	Gewährt die Berechtigung zum Erstellen eines Quellnetzwerks	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeInstances ec2:DescribeVpcs

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSourceServerForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines Quellservers	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteJob	Gewährt die Berechtigung zum Löschen eines Auftrags.	Schreiben	JobResource*		
DeleteLaunchAction	Gewährt die Berechtigung zum Löschen eines Starts	Schreiben	LaunchConfigurationTemplateResource		
			SourceServerResource		
DeleteLaunchConfigurationTemplate	Gewährt die Berechtigung zum Löschen einer Startkonfigurationsvorlage	Schreiben	LaunchConfigurationTemplateResource*		
DeleteRecoveryInstance	Gewährt die Berechtigung zum Löschen einer Wiederherstellungs-Instance	Schreiben	RecoveryInstanceResource*		
DeleteReplicationConfigurationTemplate	Gewährt die Berechtigung zum Löschen der Replikationskonfigurationsvorlage	Schreiben	ReplicationConfigurationTemplateResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteSourceNetwork	Gewährt die Berechtigung zum Löschen des Quellnetzwerks	Schreiben	SourceNetworkResource*		
DeleteSourceServer	Gewährt die Berechtigung zum Löschen des Quellservers	Write	SourceServerResource*		
DescribeJobLogItems	Gewährt die Berechtigung zur Beschreibung von Jobprotokollelementen	Read	JobResource*		
DescribeJobs	Gewährt die Berechtigung zum Beschreiben von Aufträgen	Lesen			
DescribeLaunchConfigurationTemplates	Gewährt die Berechtigung zur Beschreibung der Startkonfigurationsvorlage	Lesen			
DescribeRecoveryInstances	Gewährt die Berechtigung zum Beschreiben von Wiederherstellungs-Instances	Lesen			drs:DescribeSourceServers ec2:DescribeInstances
DescribeRecoverySnapshots	Gewährt die Berechtigung zum Beschreiben von Wiederherstellungs-Snapshots	Lesen	SourceServerResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeReplicationConfigurationTemplates	Gewährt die Berechtigung zur Beschreibung der Replikationskonfigurationsvorlage	Lesen			
DescribeReplicationServerAssociationsForDrs [nur Berechtigung]	Gewährt die Berechtigung zur Beschreibung von Replikationsservermappingen	Read			
DescribeSnapshotRequestsForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben von Snapshot-Anfragen	Lesen			
DescribeSourceNetworks	Gewährt die Berechtigung zur Beschreibung von Quellnetzwerken	Lesen			
DescribeSourceServers	Gewährt die Berechtigung zur Beschreibung von Quellservern	Lesen			
DisconnectRecoveryInstance	Gewährt die Berechtigung zum Trennen der Wiederherstellungs-Instance	Schreiben	RecoveryInstanceResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisconnectSourceServer	Gewährt die Berechtigung zum Trennen des Quellservers	Schreiben	SourceServerResource*		
ExportSourceNetworkCfnTemplate	Gewährt die Berechtigung zum Exportieren der CloudFormation-Vorlage, die Quellnetzwerkressourcen enthält	Schreiben	SourceNetworkResource*		s3:GetBucketLocation s3:GetObject s3:PutObject
				aws:RequestTag/${TagKey} aws:TagKeys	
GetAgentCommandForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen des Agent-Befehls	Read	RecoveryInstanceResource*		
			SourceServerResource*		
GetAgentConfirmedResumeInfoForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von durch Agenten bestätigten Resume-Informationen	Read	RecoveryInstanceResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			SourceServerResource*		
GetAgentInstallationAssetsForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Agenteninstallations-Assets	Read			
GetAgentReplicationInfoForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Informationen zur Agentenreplikation	Read	RecoveryInstanceResource*		
			SourceServerResource*		
GetAgentRuntimeConfigurationForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen der Agent-Laufzeitkonfiguration	Read	RecoveryInstanceResource*		
			SourceServerResource*		
GetAgentSnapshotCreditsForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Snapshots-Guthaben für Agenten	Lesen	RecoveryInstanceResource*		
			SourceServerResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetChannelCommandsForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Channel-Befehlen	Lesen			
GetFailbackCommandForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen des Failback-Befehls	Lesen	RecoveryInstanceResource*		
GetFailbackLaunchRequestedForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von angeforderten Failback-Starts	Lesen	RecoveryInstanceResource*		
GetFailbackReplicationConfiguration	Gewährt die Berechtigung zum Abrufen der Failback-Replikationskonfiguration	Lesen	RecoveryInstanceResource*		
GetLaunchConfiguration	Gewährt die Berechtigung zum Abrufen der Startkonfiguration	Read	SourceServerResource*		
GetReplicationConfiguration	Gewährt die Berechtigung zum Abrufen der Replikationskonfiguration	Lesen	SourceServerResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetSuggestedFailbackClientDeviceMappingForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen des vorgeschlagenen Failback-Client-Geräte-Mappings	Lesen	RecoveryInstanceResource*		
InitializeService	Gewährt die Berechtigung zur Initialisierung des Services	Schreiben			iam:AddRoleToInstanceProfile iam:CreateInstanceProfile iam:CreateServiceLinkedRole iam:GetInstanceProfile
IssueAgentCertificateForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Ausstellen eines Agentzertifikats	Schreiben	RecoveryInstanceResource*		
			SourceServerResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListExtensibleSourceServers	Gewährt die Berechtigung, erweiterbare Quellserver aufzulisten	Lesen			drs:DescribeSourceServers
ListLaunchActions	Gewährt die Berechtigung zum Auflisten von Starts	Lesen	LaunchConfigurationTemplateResource		
			SourceServerResource		
ListStagingAccounts	Gewährt die Berechtigung zum Auflisten von Staging-Konten	Lesen			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen			
NotifyAgentAuthenticationForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Benachrichtigen der Agentenauthentifizierung	Schreiben	RecoveryInstanceResource*		
			SourceServerResource*		
NotifyAgentConnectedForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Benachrichtigen, dass der Agent verbunden ist	Schreiben	RecoveryInstanceResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			SourceServerResource*		
NotifyAgentDisconnectedForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Benachrichtigen, dass der Agent nicht verbunden ist	Schreiben	RecoveryInstanceResource*		
			SourceServerResource*		
NotifyAgentReplicationProgressForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Benachrichtigen des Agentenreplikationsfortschritts	Schreiben	RecoveryInstanceResource*		
			SourceServerResource*		
NotifyConsistencyAttainedForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Benachrichtigen, dass Konsistenz erreicht ist	Schreiben	RecoveryInstanceResource*		
NotifyReplicationServerAuthenticationForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Benachrichtigen der Replikationsserver-Authentifizierung	Schreiben	RecoveryInstanceResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
NotifyVolumeEventForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Benachrichtigen von Replikator-Volumes	Schreiben	SourceServerResource*		
PutLaunchAction	Gewährt die Berechtigung zum Durchführen eines Starts	Schreiben	LaunchConfigurationTemplateResource		ssm:DescribeDocument
			SourceServerResource		
RetryDataReplication	Gewährt die Berechtigung zum Wiederholen der Datenreplikation	Schreiben	SourceServerResource*		
ReverseReplication	Gewährt die Berechtigung zum Umkehren der Replikation	Schreiben	RecoveryInstanceResource*		drs:DescribeReplicationConfigurationTemplates drs:DescribeSourceServers ec2:DescribeInstances

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
SendAgentLogsForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Senden von Agenten-Protokollen	Schreiben	RecoveryInstanceResource*		
			SourceServerResource*		
SendAgentMetricsForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Senden von Agenten-Metriken	Schreiben	RecoveryInstanceResource*		
			SourceServerResource*		
SendChannelCommandResultForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Senden von Channel-Befehlsergebnissen	Schreiben			
SendClientLogsForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Senden von Client-Protokollen	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SendClientMetricsForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Senden von Client-Metriken	Schreiben			
SendVolumeStatsForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Senden von Volumendurchsatzstatisti	Schreiben	SourceServerResource*		
StartFailbackLaunch	Gewährt die Berechtigung zum Starten des Failback-Starts	Schreiben	RecoveryInstanceResource*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartRecovery	Gewährt die Berechtigung zum Starten der Wiederherstellung	Schreiben	SourceServerResource*		drs:CreateRecoveryInstanceForDrs drs:ListTagsForResource ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateSnapshot

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ec2:CreateTags ec2:CreateVolume ec2:DeleteLaunchTemplateVersions ec2:DeleteSnapshot ec2:DeleteVolume ec2:DescribeAccountAttributes ec2:DescribeAvailabilityZones ec2:DescribeImages ec2:DescribeInstanceAttribute

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ec2:DescribeInstanceStatus ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSnapshots ec2:DescribeSubnets

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ec2:DescribeVolumes ec2:DetachVolume ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:RevokeSecurityGroupEgress ec2:RunInstances ec2:StartInstances ec2:StopInstances ec2:TerminateInstances

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
StartReplication	Gewährt die Berechtigung zum Starten der Replikation	Schreiben	SourceServerResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartSourceNetworkRecovery	Gewährt die Berechtigung zum Starten der Netzwerkwiederherstellung	Schreiben	SourceNetworkResource*		cloudformation:CreateStack cloudformation:DescribeStackResource cloudformation:DescribeStacks cloudformation:UpdateStack drs:GetLaunchConfiguration ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunch

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					Templates ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:ModifyLaunchTemplate s3:GetObject s3:PutObject
				aws:RequestTag/${TagKey} aws:TagKeys	
StartSourceNetworkReplication	Gewährt die Berechtigung zum Starten der Netzwerkreplikation	Schreiben	SourceNetworkResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopFailback	Gewährt die Berechtigung zum Stoppen des Failbacks	Schreiben	RecoveryInstanceResource*		
StopReplication	Gewährt die Berechtigung zum Beenden der Replikation	Schreiben	SourceServerResource*		
StopSourceNetworkReplication	Gewährt die Berechtigung zum Stoppen der Netzwerkreplikation	Schreiben	SourceNetworkResource*		
TagResource	Gewährt die Berechtigung zum Zuordnen eines Ressourcen-Tags.	Markierung	JobResource		
			LaunchConfigurationTemplateResource		
			RecoveryInstanceResource		
			ReplicationConfigurationTemplateResource		
			SourceNetworkResource		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			SourceServerResource		
				aws:RequestTag/${TagKey} aws:TagKeys drs:CreateAction	
TerminateRecoveryInstances	Gewährt die Berechtigung zum Beenden von Wiederherstellungs-Instances	Schreiben	RecoveryInstanceResource*		drs:DescribeSourceServers ec2:DeleteVolume ec2:DescribeInstances ec2:DescribeVolumes ec2:TerminateInstances

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Markieren	JobResource		
			LaunchConfigurationTemplateResource		
			RecoveryInstanceResource		
			ReplicationConfigurationTemplateResource		
			SourceNetworkResource		
			SourceServerResource		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
UpdateAgentBacklogForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren des Agenten-Backlog	Schreiben	RecoveryInstanceResource*		
			SourceServerResource*		
UpdateAgentConversionInfoForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren von Agentenkonvertierungsinformationen	Schreiben	RecoveryInstanceResource*		
			SourceServerResource*		
UpdateAgentReplicationInfoForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren von Agentenreplikationsinformationen	Schreiben	RecoveryInstanceResource*		
			SourceServerResource*		
UpdateAgentReplicationProcessStateForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren des Status des Agentenreplikationsprozesses	Schreiben	RecoveryInstanceResource*		
			SourceServerResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateAgentSourcePropertiesForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren von Quelleneigenschaften für Agenten	Schreiben	RecoveryInstanceResource*		
			SourceServerResource*		
UpdateFailbackClientDeviceMappingForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren des Failback-Client-Geräte-Mappings	Schreiben	RecoveryInstanceResource*		
UpdateFailbackClientLastSeenForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren des zuletzt gesehenen Failback-Clients	Schreiben	RecoveryInstanceResource*		
UpdateFailbackReplicationConfiguration	Gewährt die Berechtigung zum Aktualisieren der Failback-Replikationskonfiguration	Schreiben	RecoveryInstanceResource*		
UpdateLaunchConfiguration	Gewährt die Berechtigung zum Aktualisieren einer Startkonfiguration	Schreiben	SourceServerResource*		ec2:DescribeInstances

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateLaunchConfigurationTemplate	Gewährt die Berechtigung zum Aktualisieren einer Startkonfiguration	Schreiben	LaunchConfigurationTemplateResource*		
UpdateReplicationCertificateForDrs [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren eines Replikationszertifikats	Schreiben	RecoveryInstanceResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateReplicationConfiguration	Gewährt die Berechtigung zum Aktualisieren der Replikationskonfiguration	Schreiben	SourceServerResource*		ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetEbsDefaultKmsKeyId ec2:GetEbsEncryptionByDefault kms:CreateGrant kms:DescribeKey

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateReplicationConfigurationTemplate	Gewährt die Berechtigung zum Aktualisieren der Replikationskonfigurationsvorlage	Schreiben	ReplicationConfigurationTemplateResource*		ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetEbsDefaultKmsKeyId ec2:GetEbsEncryptionByDefault kms:CreateGrant kms:DescribeKey

Von AWS Elastic Disaster Recovery definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
JobResource	`arn:${Partition}:drs:${Region}:${Account}:job/${JobID}`	aws:ResourceTag/${TagKey}
RecoveryInstanceResource	`arn:${Partition}:drs:${Region}:${Account}:recovery-instance/${RecoveryInstanceID}`	aws:ResourceTag/${TagKey} drs:EC2InstanceARN
ReplicationConfigurationTemplateResource	`arn:${Partition}:drs:${Region}:${Account}:replication-configuration-template/${ReplicationConfigurationTemplateID}`	aws:ResourceTag/${TagKey}
LaunchConfigurationTemplateResource	`arn:${Partition}:drs:${Region}:${Account}:launch-configuration-template/${LaunchConfigurationTemplateID}`	aws:ResourceTag/${TagKey}
SourceServerResource	`arn:${Partition}:drs:${Region}:${Account}:source-server/${SourceServerID}`	aws:ResourceTag/${TagKey}
SourceNetworkResource	`arn:${Partition}:drs:${Region}:${Account}:source-network/${SourceNetworkID}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Elastic Disaster Recovery

AWS Elastic Disaster Recovery definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um

die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString
drs:CreateAction	Filtert den Zugriff nach Name einer ressourcenerstellenden API-Aktion	Zeichenfolge
drs:EC2InstanceARN	Filtert den Zugriff nach der EC2-Instance, von der die Anforderung stammt	ARN

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Elastic File System

Amazon Elastic File System (Servicepräfix: `elasticfilesystem`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Elastic File System definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Backup [nur Berechtigung]	Gewährt die Berechtigung zum Starten einer Backup-Aufgabe für ein bestehendes Dateisystem	Write	file-system*		
ClientMount [nur Berechtigung]	Gewährt die Berechtigung, einem NFS-Client Lesezugriff auf ein Dateisystem zu geben	Read	file-system*		
				elasticfilesystem:AccessPointArn elasticfilesystem:AccessedViaMountTarget	
ClientRootAccess [nur Berechtigung]	Gewährt die Berechtigung, einem NFS-Client Root-Zugriff auf ein Dateisystem zu geben	Write	file-system*		
				elasticfilesystem:AccessPointArn	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				elasticfilesystem:AccessedViaMountTarget	
ClientWrite [nur Berechtigung]	Gewährt die Berechtigung, einem NFS-Client Schreibzugriff auf ein Dateisystem zu geben	Write	file-system*		
				elasticfilesystem:AccessPointArn elasticfilesystem:AccessedViaMountTarget	
CreateAccessPoint	Gewährt die Berechtigung zum Erstellen eines Zugriffspunkts für das angegebene Dateisystem	Write	file-system*		elasticfilesystem:TagResource
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateFileSystem	Gewährt die Berechtigung zum Erstellen eines neuen, leeren Dateisystems	Write		aws:RequestTag/${TagKey} aws:TagKeys elasticfilesystem:Encrypted	elasticfilesystem:TagResource
CreateMountTarget	Gewährt die Berechtigung zum Erstellen eines Mounting-Ziels für ein Dateisystem	Schreiben	file-system*		
CreateReplicationConfiguration	Gewährt die Berechtigung zum Erstellen einer neuen Replikationskonfiguration	Schreiben	file-system*		
CreateTags	Erteilt die Berechtigung, einem Dateisystem zugeordnete Tags zu erstellen oder zu überschreiben; veraltet, siehe TagResource	Tagging	file-system*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessPoint	Gewährt die Berechtigung zum Löschen des angegebenen Zugriffspunkts	Write	access-point*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteFileSystem	Gewährt die Berechtigung zum Löschen eines Dateisystems, wobei der Zugriff auf seinen Inhalt dauerhaft unterbrochen wird	Write	file-system*		
DeleteFileSystemPolicy	Gewährt die Berechtigung zum Löschen der Richtlinie auf Ressourcenebene für ein Dateisystem	Berechtigungsverwaltung	file-system*		
DeleteMountTarget	Gewährt die Berechtigung zum Löschen des angegebenen Mounting-Ziels	Schreiben	file-system*		
DeleteReplicationConfiguration	Gewährt die Berechtigung zum Löschen einer Replikationskonfiguration	Schreiben	file-system*		
DeleteTags	Erteilt die Berechtigung, die angegebenen Tags aus einem Dateisystem zu löschen; veraltet, siehe UntagResource	Tagging	file-system*		
				aws:TagKeys	
DescribeAccessPoints	Gewährt die Berechtigung zum Anzeigen der Beschreibungen von Amazon EFS-Zugriffspunkten	List	access-point		
			file-system		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeAccountPreferences	Gewährt die Berechtigung zum Anzeigen der für ein Konto geltenden Kontoeinstellungen	Auflisten			
DescribeBackupPolicy	Erteilt die Berechtigung, das BackupPolicy Objekt für ein Amazon EFS-Dateisystem anzuzeigen	Lesen	file-system*		
DescribeFileSystemPolicy	Gewährt die Berechtigung zum Anzeigen der Richtlinie auf Ressourcenebene für ein Amazon EFS-Dateisystem	Lesen	file-system		
DescribeFileSystems	Erteilt die Berechtigung, die Beschreibung eines Amazon EFS-Dateisystems, spezifiziert nach Dateisystem CreationToken oder FileSystemId; oder die Beschreibung aller Dateisysteme, die dem Aufrufer gehören, AWS-Konto in der AWS Region des aufgerufenen Endpunkts anzuzeigen	Auflisten	file-system		
DescribeLifecycleConfiguration	Erteilt die Berechtigung, das LifecycleConfiguration Objekt für ein Amazon EFS-Dateisystem anzuzeigen	Lesen	file-system*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeMountTargetSecurityGroups	Gewährt die Berechtigung zum Anzeigen der Sicherheitsgruppen, die für ein Mounting-Ziel aktiv sind	Read	file-system*		
DescribeMountTargets	Gewährt die Berechtigung zum Anzeigen der Beschreibungen aller Mounting-Ziele oder eines bestimmten Mounting-Ziels für ein Dateisystem	Lesen	file-system* access-point		
DescribeReplicationConfigurations	Erteilt die Berechtigung, die Beschreibung einer Amazon EFS-Replikationskonfiguration anzuzeigen, die von angegeben wurde FileSystemId, oder die Beschreibung aller Replikationskonfigurationen, die den Anrufern gehören, AWS-Konto in der AWS Region des Endpunkts, der aufgerufen wird, einzusehen.	Auflisten	file-system		
DescribeTags	Gewährt die Berechtigung zum Anzeigen der einem Dateisystem zugeordneten Tags	Read	file-system*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Anzeigen der Tags, die der angegebenen Amazon EFS-Ressource zugeordnet sind	Read	access-point		
			file-system		
ModifyMountTargetSecurityGroups	Gewährt die Berechtigung zum Ändern der Gruppe von Sicherheitsgruppen, die für ein Mounting-Ziel aktiv sind	Write	file-system*		
PutAccountPreferences	Gewährt die Berechtigung zum Festlegen der Kontoeinstellungen eines Kontos	Schreiben			
PutBackupPolicy	Erteilt die Berechtigung, automatische Backups mit AWS Backup zu aktivieren oder zu deaktivieren, indem ein neues BackupPolicy Objekt erstellt wird	Schreiben	file-system*		
PutFileSystemPolicy	Gewährt die Berechtigung zum Anwenden einer Richtlinie auf Ressourcenebene, die die Aktionen definiert, die bestimmten Akteuren für das angegebene Dateisystem erlaubt oder verweigert werden	Berechtigungsverwaltung	file-system*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutLifecycleConfiguration	Erteilt die Berechtigung, das Lebenszyklusmanagement durch Erstellen eines neuen LifecycleConfiguration Objekts zu aktivieren	Schreiben	file-system*		
Restore [nur Berechtigung]	Gewährt die Berechtigung zum Starten einer Wiederherstellungsaufgabe für ein Backup eines Dateisystems	Write	file-system*		
TagResource	Gewährt die Berechtigung zum Erstellen oder Überschreiben der Tags, die der angegebenen Amazon EFS-Ressource zugeordnet sind	Markieren	access-point		
			file-system		
				aws:RequestTag/${TagKey} aws:TagKeys elasticfilesystem:CreateAction	
UntagResource	Gewährt die Berechtigung zum Löschen der angegebenen Tags aus einer Amazon EFS-Ressource	Markieren	access-point		
			file-system		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
UpdateFileSystem	Gewährt die Berechtigung zum Aktualisieren des Durchsatzmodus oder des bereitgestellten Durchsatzvolumens eines vorhandenen Dateisystems	Schreiben	file-system*		
UpdateFileSystemProtection	Gewährt die Berechtigung zum Aktualisieren des Dateisystemschutzes eines vorhandenen Dateisystems	Schreiben	file-system*		

Von Amazon Elastic File System definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
file-system	`arn:${Partition}:elasticfilesystem:${Region}:${Account}:file-system/${FileSystemId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
access-point	`arn:${Partition}:elasticfilesystem:${Region}:${Account}:access-point/${AccessPointId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Elastic File System

Amazon Elastic File System definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wertepaaren, die in der Anforderung zulässig sind	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paar einer Ressource	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach Liste von Tag-Schlüsseln, die in der Anforderung zulässig sind	ArrayOfString
elasticfilesystem:AccessPointArn	Filtert den Zugriff nach dem ARN des Zugriffspunkts, der zum Mounten des Dateisystems verwendet wird	ARN
elasticfilesystem:AccessedViaMountTarget	Filtert den Zugriff in Bezug darauf, ob über Mounting-Ziele auf das Dateisystem zugegriffen wird	Bool

Bedingungsschlüssel	Beschreibung	Typ
elasticfilesystem:CreateAction	Filtert den Zugriff nach Name einer ressourcenerstellenden API-Aktion	String
elasticfilesystem:Encrypted	Filtert den Zugriff in Bezug darauf, ob Benutzer nur verschlüsselte oder unverschlüsselte Dateisysteme erstellen können	Bool

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Elastic Inference

Amazon Elastic Inference (Servicepräfix: `elastic-inference`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Elastic Inference definierte Aktionen
- Von Amazon Elastic Inference definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Elastic Inference

Von Amazon Elastic Inference definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den

Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Connect	Gewährt dem Kunden die Erlaubnis zur Verbindung mit Elastic Inference Accelerator	Write	accelerator*		
DescribeAcceleratorOfferings	Gewährt die Berechtigung zur Beschreibung der Standorte, an denen ein bestimmter Accelerator-Typ oder eine bestimmte Gruppe von Typen in einer bestimmten Region vorhanden ist	List			
DescribeAcceleratorTypes	Gewährt die Erlaubnis, die in einer bestimmten Region verfügbaren Accelerator-Typen sowie deren Eigenschaften wie Speicher und Durchsatz zu beschreiben	List			
DescribeAccelerators	Gewährt die Erlaubnis, Informationen über einen bereitgestellten Satz von Acceleratoren zu beschreiben, die zu einem Konto gehören	List			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten aller Tags auf einer Amazon RDS-Ressource	Read			
TagResource	Gewährt die Berechtigung, der angegebenen QuickSight-Ressource ein oder mehrere	Markieren			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Tags (Schlüsselwertpaare) zuzuweisen				
UntagResource	Gewährt die Berechtigung zum Löschen eines oder mehrerer Tags aus einer Ressource	Markieren			

Von Amazon Elastic Inference definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
accelerator	`arn:${Partition}:elastic-inference:${Region}:${Account}:elastic-inference-accelerator/${AcceleratorId}`	

Bedingungsschlüssel für Amazon Elastic Inference

EI besitzt keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für den Amazon Elastic Kubernetes Service

Amazon Elastic Kubernetes Service (Service-Präfix: `eks`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Elastic Kubernetes Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie

den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AccessKubernetesApi [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen von Kubernetes-Objekten über die AWS-EKS-Konsole	Lesen	cluster*		
AssociateAccessPolicy	Gewährt die Berechtigung, einem Amazon-EKS-Zugriffseintrag eine Amazon-EKS-Zugriffsrichtlinie zuzuordnen	Schreiben	access-entry*		
				eks:policyArn eks:namespaces	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				eks:accessScope	
AssociateEncryptionConfig	Gewährt die Berechtigung zum Zuordnen der Verschlüsselungskonfiguration zu einem Cluster	Write	cluster*		
AssociateIdentityProviderConfig	Gewährt die Berechtigung zum Zuordnen einer Identitätsanbieter-Konfiguration zu einem Cluster	Schreiben	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys eks:clientId eks:issuerUrl	
CreateAccessEntry	Gewährt die Berechtigung zum Erstellen eines Amazon-EKS-Zugriffseintrags	Schreiben	cluster*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys eks:principalArn eks:kubernetesGroups eks:username eks:accessEntryType	
CreateAddon	Gewährt die Berechtigung zum Erstellen eines Amazon EKS-Add-ons	Write	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCluster	Gewährt die Berechtigung zum Erstellen eines Amazon EKS-Clusters	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys eks:bootstrapClusterCreatorAdminPermissions	
CreateEksAnywhereSubscription	Gewährt die Berechtigung zum Erstellen eines EKS-Anywhere-Abonnements	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFargateProfile	Gewährt die Berechtigung zum Erstellen eines AWS-Fargate-Profils	Write	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNodegroup	Gewährt die Berechtigung zum Erstellen einer Amazon EKS-Knotengruppe	Schreiben	cluster*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePodIdentityAssociation	Gewährt die Berechtigung zum Erstellen einer EKS-Pod-Identity-Zuordnung	Schreiben	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessEntry	Gewährt die Berechtigung zum Löschen eines Amazon-EKS-Zugriffseintrags	Schreiben	access-entry*		
DeleteAddon	Gewährt die Berechtigung zum Löschen eines Amazon EKS-Add-Ons	Write	addon*		
DeleteCluster	Gewährt die Berechtigung zum Löschen eines Amazon EKS-Clusters	Schreiben	cluster*		
DeleteEksAnywhereSubscription	Gewährt die Berechtigung zum Beschreiben eines EKS-Anywhere-Abonnements	Schreiben	eks-anywhere-subscription*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteFargateProfile	Gewährt die Berechtigung zum Löschen eines AWS-Fargate-Profils	Write	fargateprofile*		
DeleteNodegroup	Gewährt die Berechtigung zum Löschen einer Amazon EKS-Knotengruppe	Schreiben	nodegroup*		
DeletePodIdentityAssociation	Gewährt die Berechtigung zum Löschen einer EKS-Pod-Identity-Zuordnung	Schreiben	podidentityassociation*		
DeregisterCluster	Gewährt die Berechtigung zur Aufhebung der Registrierung eines externen Clusters	Schreiben	cluster*		
DescribeAccessEntry	Gewährt die Berechtigung zum Beschreiben eines Amazon-EKS-Zugriffseintrags	Lesen	access-entry*		
DescribeAddon	Gewährt die Berechtigung zum Abrufen beschreibender Informationen zu einem Amazon EKS-Add-On	Lesen	addon*		
DescribeAddonConfiguration	Gewährt die Berechtigung zum Auflisten von Konfigurationsoptionen über ein Amazon-EKS-Add-on	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeAddonVersions	Gewährt die Berechtigung zum Abrufen beschreibender Versionsinformationen zu den von Amazon EKS-Add-Ons unterstützten Add-Ons	Read			
DescribeCluster	Gewährt die Berechtigung zum Abrufen beschreibender Informationen zu einen Amazon EKS-Cluster	Lesen	cluster*		
DescribeEksAnywhereSubscription	Gewährt die Berechtigung zum Beschreiben eines EKS-Anywhere-Abonnements	Lesen	eks-anywhere-subscription*		
DescribeFargateProfile	Gewährt die Berechtigung zum Abrufen beschreibender Informationen über ein AWS-Fargate-Profil, das einem Cluster zugeordnet ist	Read	fargateprofile*		
DescribeIdentityProviderConfig	Gewährt die Berechtigung zum Abrufen beschreibender Informationen zu einer Idp-Konfiguration, die einem Cluster zugeordnet ist	Lesen	identityproviderconfig*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeInsight	Gewährt die Berechtigung zum Abrufen beschreibender Informationen zu einem erkannten Insight für einen angegebenen Cluster	Lesen	cluster*		
DescribeNodegroup	Gewährt die Berechtigung zum Abrufen beschreibender Informationen zu einer Amazon EKS-Knotengruppe	Lesen	nodegroup*		
DescribePodIdentityAssociation	Gewährt die Berechtigung zum Beschreiben einer EKS-Pod-Identity-Zuordnung	Lesen	podidentityassociation*		
DescribeUpdate	Gewährt die Berechtigung zum Abrufen eines bestimmten Updates für eine(n) bestimmte(n) Amazon EKS-Cluster/-Knotengruppe/-Add-On (in der angegebenen oder standardmäßigen Region)	Lesen	cluster*		
			addon		
			nodegroup		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateAccessPolicy	Gewährt die Berechtigung zum Trennen einer Amazon-EKS-Zugriffsrichtlinie von einem Amazon-EKS-Zugriffseintrag	Schreiben	access-entry*		
				eks:policyArn eks:namespaces eks:accessScope	
DisassociateIdentityProviderConfig	Gewährt die Berechtigung zum Löschen einer zugeordneten Idp-Konfiguration	Schreiben	identityproviderconfig*		
ListAccessEntries	Gewährt die Berechtigung zum Auflisten aller Amazon-EKS-Zugriffseinträge	Auflisten	cluster*		
ListAccessPolicies	Gewährt die Berechtigung zum Auflisten von Amazon-EKS-Zugriffsrichtlinien	Auflisten			
ListAddons	Gewährt die Berechtigung zum Auflisten der Amazon-EKS-Add-Ons in Ihrem AWS-Konto (in der angegebenen oder standardmäßigen Region) für einen bestimmten Cluster	Auflisten	cluster*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAssociatedAccessPolicies	Gewährt die Berechtigung zum Auflisten einer einem Amazon-EKS-Zugriffseintrag zugewiesenen Amazon-EKS-Zugriffsrichtlinie	Auflisten	access-entry*		
ListClusters	Gewährt die Berechtigung zum Auflisten der Amazon-EKS-Cluster im AWS-Konto (in der angegebenen oder der Standardregion)	Auflisten			
ListEksAnywhereSubscriptions	Gewährt die Berechtigung zum Auflisten von EKS-Anywhere-Abonnements	Auflisten			
ListFargateProfiles	Gewährt die Berechtigung zum Auflisten der AWS-Fargate-Profile in Ihrem AWS-Konto (in der angegebenen oder der Standardregion), die mit einem bestimmten Cluster verbunden sind	List	cluster*		
ListIdentityProviderConfigs	Gewährt die Berechtigung zum Auflisten der Idp-Konfigurationen in Ihrem AWS-Konto (in der angegebenen oder der Standardregion), die mit einem bestimmten Cluster verbunden sind	Auflisten	cluster*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListInsights	Gewährt die Berechtigung zum Auflisten aller erkannten Insights für einen angegebenen Cluster	Auflisten	cluster*		
ListNodegroups	Gewährt die Berechtigung zum Auflisten der Amazon-EKS-Knotengruppen in Ihrem AWS-Konto (in der angegebenen oder standardmäßigen Region), die einem bestimmten Cluster angefügt sind	Auflisten	cluster*		
ListPodIdentityAssociations	Gewährt die Berechtigung zum Auflisten von EKS-Pod Identity-Zuordnungen	Auflisten	cluster*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für die angegebene Ressource	Read	addon		
			cluster		
			eks-anywhere-subscription		
			fargateprofile		
			identityproviderconfig		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			nodegroup		
ListUpdates	Gewährt die Berechtigung zum Auflisten der Updates für eine(n) bestimmte(n) Amazon EKS-Cluster/-Knotengruppe/-Add-On (in der angegebenen oder standardmäßigen Region)	Auflisten	cluster*		
			addon		
			nodegroup		
RegisterCluster	Gewährt die Berechtigung zur Registrierung eines externen Clusters	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Gewährt die Berechtigung zum Markieren der angegebenen Ressource	Markieren	access-entry		
			addon		
			cluster		
			eks-anywhere-subscription		
			fargateprofile		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			identityproviderconfig		
			nodegroup		
			podidentityassociation		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung der angegebenen Ressource	Tagging	access-entry		
			addon		
			cluster		
			eks-anywhere-subscription		
			fargateprofile		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			identityproviderconfig		
			nodegroup		
			podidentityassociation		
				aws:TagKeys	
UpdateAccessEntry	Gewährt die Berechtigung zum Aktualisieren eines Amazon-EKS-Zugriffseintrags	Schreiben	access-entry*		
UpdateAddon	Gewährt die Berechtigung zum Aktualisieren von Amazon EKS-Add-On-Konfigurationen wie der VPC-CNI-Version	Write	addon*		
UpdateClusterConfig	Gewährt die Berechtigung zum Aktualisieren von Amazon EKS-Cluster-Konfigurationen (z. B. API-Server-Endpunktzugriff)	Write	cluster*		
UpdateClusterVersion	Gewährt die Berechtigung zum Aktualisieren der Kubernetes-Version eines Amazon EKS-Clusters	Schreiben	cluster*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateEksAnywhereSubscription	Gewährt die Berechtigung zum Aktualisieren eines EKS-Anywhere-Abonnements	Schreiben	eks-anywhere-subscription*		
UpdateNodegroupConfig	Gewährt die Berechtigung zum Aktualisieren der Konfigurationen der Amazon EKS-Knotengruppen (z. B.: min./max./gewünschte Kapazität oder Bezeichnungen)	Write	nodegroup*		
UpdateNodegroupVersion	Gewährt die Berechtigung zum Aktualisieren der Kubernetes-Version einer Amazon EKS-Knotengruppe	Schreiben	nodegroup*		
UpdatePodIdentityAssociation	Gewährt die Berechtigung zum Aktualisieren einer EKS-Pod-Identity-Zuordnung	Schreiben	podidentityassociation*		

Von Amazon Elastic Kubernetes Service definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
cluster	arn:${Partition}:eks:${Region}:${Account}:cluster/${ClusterName}	aws:ResourceTag/${TagKey}
nodegroup	arn:${Partition}:eks:${Region}:${Account}:nodegroup/${ClusterName}/${NodegroupName}/${UUID}	aws:ResourceTag/${TagKey}
addon	arn:${Partition}:eks:${Region}:${Account}:addon/${ClusterName}/${AddonName}/${UUID}	aws:ResourceTag/${TagKey}
fargateprofile	arn:${Partition}:eks:${Region}:${Account}:fargateprofile/${ClusterName}/${FargateProfileName}/${UUID}	aws:ResourceTag/${TagKey}
identityproviderconfig	arn:${Partition}:eks:${Region}:${Account}:identityproviderconfig/${ClusterName}/${IdentityProviderType}/${IdentityProviderConfigName}/${UUID}	aws:ResourceTag/${TagKey}
eks-anywhere-subscription	arn:${Partition}:eks:${Region}:${Account}:eks-anywhere-subscription/${UUID}	aws:ResourceTag/${TagKey}
podidentityassociation	arn:${Partition}:eks:${Region}:${Account}:podidentityassociation/${ClusterName}/${UUID}	aws:ResourceTag/${TagKey}
access-entry	arn:${Partition}:eks:${Region}:${Account}:access-entry/${ClusterName}/${IamIdentityType}/${IamIdentityAccountID}/${IamIdentityName}/${UUID}	aws:ResourceTag/${TagKey} eks:accessEntryType eks:clusterName

Ressourcentypen	ARN	Bedingungsschlüssel
		eks:kubernetesGroups eks:principalArn eks:username
access-policy	`arn:${Partition}:eks::aws:cluster-access-policy/${AccessPolicyName}`	

Bedingungsschlüssel für Amazon Elastic Kubernetes Service

Amazon Elastic Kubernetes Service definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff entsprechend eines Schlüssels, der in der Anforderung vorhanden ist, die der Benutzer an den EKS-Service sendet	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff anhand eines Tag-Schlüssel-Wert-Paares	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach der Liste aller Tag-Schlüsselnamen, die in der Anforderung vorhanden sind, die der Benutzer an den EKS-Service sendet	ArrayOfString

Bedingungsschlüssel	Beschreibung	Typ
eks:accessEntryType	Filtert den Zugriff nach dem Zugriffseintragstyp, der in den Zugriffseintragsanforderungen vorhanden ist, die der Benutzer an den EKS-Service sendet	String
eks:accessScope	Filtert den Zugriff nach dem accessScope, der in den Anforderungen des Benutzers an den EKS-Dienst zum Zuweisen/Trennen von Zugriffsrichtlinien enthalten ist	String
eks:bootstrapClusterCreatorAdminPermissions	Filtert den Zugriff nach dem in der Anforderung zum Erstellen eines Clusters bootstrapClusterCreatorAdminPermissions vorhandenen	Bool
eks:clientId	Filtert den Zugriff nach der clientId, die in der associate IdentityProviderKonfigurationsanforderung vorhanden ist, die der Benutzer an den EKS-Service sendet	String
eks:clusterName	Filtert den Zugriff nach dem clusterName, der in den Zugriffseintragsanforderungen vorhanden ist, die der Benutzer an den EKS-Service sendet	String
eks:issuerUrl	Filtert den Zugriff nach der issuerUrl, die in der associate IdentityProviderKonfigurationsanforderung vorhanden ist, die der Benutzer an den EKS-Service sendet	String
eks:kubernetesGroups	Filtert den Zugriff nach den kubernetesGroups, die in den Zugriffseintragsanforderungen vorhanden sind, die der Benutzer an den EKS-Service sendet	ArrayOfString
eks:namespaces	Filtert den Zugriff nach den Namespaces, die in den Anforderungen des Benutzers an den EKS-Dienst zum Zuweisen/Trennen von Zugriffsrichtlinien enthalten sind	ArrayOfString

Bedingungsschlüssel	Beschreibung	Typ
eks:policyArn	Filtert den Zugriff nach dem policyArn, der in den Zugriffseintragsanforderungen vorhanden ist, die der Benutzer an den EKS-Service sendet	ARN
eks:principalArn	Filtert den Zugriff nach dem porincipalArn, der in den Zugriffseintragsanforderungen vorhanden ist, die der Benutzer an den EKS-Service sendet	ARN
eks:username	Filtert den Zugriff nach dem Kubernetes-Benutzernamen, der in den Zugriffseintragsanforderungen vorhanden ist, die der Benutzer an den EKS-Service sendet	String

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elastic Load Balancing

AWS Elastic Load Balancing (Servicepräfix: `elasticloadbalancing`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Elastic Load Balancing definierte Aktionen
- Von AWS Elastic Load Balancing definierte Ressourcentypen
- Bedingungsschlüssel für AWS Elastic Load Balancing

Von AWS Elastic Load Balancing definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddTags	Gewährt die Berechtigung zum Hinzufügen der angegebenen Tags zum angegebenen Load Balancer. Jeder Load Balancer kann maximal 10 Tags aufweisen.	Markierung	loadbalancer*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:CreateAction	
ApplySecurityGroupsToLoadBalancer	Gewährt die Berechtigung zum Zuordnen einzelner oder mehrerer Sicherheitsgruppen zu Ihrem Load Balancer in einer Virtual Private Cloud (VPC).	Schreiben	loadbalancer*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup	
AttachLoadBalancerToSubnets	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Subnetze zum Satz der konfigurierten Subnetze für den angegebenen Load Balancer.	Schreiben	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:Subnet	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ConfigureHealthCheck	Gewährt die Berechtigung zum Angeben der Zustandsprüfungseinstellungen, die zum Auswerten des Zustands von Backend-Instances verwenden werden sollen.	Schreiben	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateAppCookieStickinessPolicy	Gewährt die Berechtigung zum Generieren einer Richtlinie für Sticky Sessions mit Gültigkeitsdauerwerten für Sticky Sessions, die denen eines anwendungsgenerierten Cookies entsprechen.	Schreiben	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateLBCookieStickinessPolicy	Gewährt die Berechtigung zum Generieren einer Richtlinie für Sticky Sessions mit Gültigkeitsdauerwerten für Sticky Sessions, die von der Gültigkeitsdauer des Browsers (Benutzer-Agent) oder einer festgelegten Ablaufzeit abhängig sind.	Schreiben	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateLoadBalancer	Gewährt die Berechtigung zum Erstellen eines Load Balancers	Schreiben	loadbalancer		elasticloadbalancing:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup elasticloadbalancing:Subnet elasticloadbalancing:Scheme elasticloadbalancing:Listen	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				elasticloadbalancing:ListenerProtocol	
CreateLoadBalancerListeners	Gewährt die Berechtigung zum Erstellen einzelner oder mehrerer Listener für den angegebenen Load Balancer.	Schreiben	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:ListenerProtocol	
CreateLoadBalancerPolicy	Gewährt die Berechtigung zum Erstellen einer Richtlinie mit den angegebenen Attributen für den angegebenen Load Balancer.	Schreiben	loadbalancer*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy	
DeleteLoadBalancer	Gewährt die Berechtigung zum Löschen des angegebenen Load Balancers.	Schreiben	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteLoadBalancerListeners	Gewährt die Berechtigung zum Löschen der angegebenen Listener aus dem angegebenen Load Balancer.	Schreiben	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteLoadBalancerPolicy	Gewährt die Berechtigung zum Löschen der angegebenen Richtlinie aus dem angegebenen Load Balancer. Diese Richtlinie darf für keinen Listener aktiviert werden.	Schreiben	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeregisterInstancesFromLoadBalancer	Gewährt die Berechtigung zum Aufheben der Registrierung der angegebenen Instances aus dem angegebenen Load Balancer.	Schreiben	loadbalancer*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DescribeInstanceHealth	Gewährt die Berechtigung zum Beschreiben des Status der angegebenen Instances im Hinblick auf den angegebenen Load Balancer.	Lesen			
DescribeLoadBalancerAttributes	Gewährt die Berechtigung zum Beschreiben der Attribute für den angegebenen Load Balancer.	Lesen			
DescribeLoadBalancerPolicies	Gewährt die Berechtigung zum Beschreiben des angegebenen Richtlinien.	Lesen			
DescribeLoadBalancerPolicyTypes	Gewährt die Berechtigung zum Beschreiben der angegebenen Load-Balancer-Richtlinientypen.	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeLoadBalancers	Gewährt die Berechtigung zum Beschreiben der angegebenen Load Balancer. Wenn keine Load Balancer angegeben werden, beschreibt der Aufruf alle Ihre Load Balancer.	Auflisten			
DescribeTags	Gewährt die Berechtigung zum Beschreiben der den angegebenen Load Balancern zugeordneten Tags.	Lesen			
DetachLoadBalancerFromSubnets	Gewährt die Berechtigung zum Entfernen der angegebenen Subnetze aus dem Satz der für den Load Balancer konfigurierten Subnetze.	Schreiben	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisableAvailabilityZonesForLoadBalancer	Gewährt die Berechtigung zum Entfernen der angegebenen Availability Zones aus dem Satz der Availability Zones für den angegebenen Load Balancer.	Schreiben	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
EnableAvailabilityZonesForLoadBalancer	Gewährt die Berechtigung zum Hinzufügen der angegebenen Availability Zones zum Satz der Availability Zones für den angegebenen Load Balancer.	Schreiben	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyLoadBalancerAttributes	Gewährt die Berechtigung zum Ändern der Attribute für den angegebenen Load Balancer.	Schreiben	loadbalancer*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RegisterInstancesWithLoadBalancer	Gewährt die Berechtigung zum Hinzufügen der angegebenen Instances zum angegebenen Load Balancer.	Schreiben	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveTags	Gewährt die Berechtigung zum Entfernen eines oder mehrerer Tags aus dem angegebenen Load Balancer.	Markierung	loadbalancer*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetLoadBalancerListenerSSLCertificate	Gewährt die Berechtigung zum Festlegen des Zertifikats, das die SSL-Verbindungen des angegebenen Listeners beendet.	Schreiben	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SetLoadBalancerPoliciesForBackendServer	Gewährt die Berechtigung zum Ersetzen des Satzes von Richtlinien, die dem angegebenen Port zugeordnet sind, den der Backend-Server überwacht, durch einen neuen Satz von Richtlinien.	Schreiben	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetLoadBalancerPoliciesOfListener	Gewährt die Berechtigung zum Ersetzen des aktuellen Satzes von Richtlinien für den angegebenen Load Balancer-Port durch den angegebenen Satz von Richtlinien.	Schreiben	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy	

Von AWS Elastic Load Balancing definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
loadbalancer	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/${LoadBalancerName}`	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Elastic Load Balancing

AWS Elastic Load Balancing definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wertepaaren, die in der Anforderung zulässig sind	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paar einer Ressource	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach Liste von Tag-Schlüsseln, die in der Anforderung zulässig sind	ArrayOfString
elasticloadbalancing:CreateAction	Filtert den Zugriff nach Name einer ressourcenerstellenden API-Aktion	Zeichenfolge
elasticloadbalancing:ListenerProtocol	Filtert den Zugriff durch die Listener-Protokolle, die in der Anfrage zulässig sind	ArrayOfString
elasticloadbalancing:ResourceTag/	Filtert den Zugriff nach vorangestellter Zeichenfolge eines Tag-Schlüssel/Wertepaars, das an eine Ressource angefügt ist	Zeichenfolge
elasticloadbalancing:ResourceTag/${TagKey}	Filtert den Zugriff nach vorangestellter Zeichenfolge eines Tag-Schlüssel/Wertepaars, das an eine Ressource angefügt ist	Zeichenfolge
elasticloadbalancing:Scheme	Filtert den Zugriff nach dem Load Balancer-Schema, das in der Anforderung zulässig ist	Zeichenfolge
elasticloadbalancing:SecurityGroup	Filtert den Zugriff durch die Sicherheitsgruppen-IDs, die in der Anforderung zulässig sind	ArrayOfString

Bedingungsschlüssel	Beschreibung	Typ
elasticloadbalancing:SecurityPolicy	Filtert den Zugriff durch die SSL-Sicherheitsrichtlinien, die in der Anfrage zulässig sind	ArrayOfString
elasticloadbalancing:Subnet	Filtert den Zugriff durch die Subnetz-IDs, die in der Anfrage zulässig sind	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elastic Load Balancing V2

AWS Elastic Load Balancing V2 (Servicepräfix: `elasticloadbalancing`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Elastic Load Balancing V2 definierte Aktionen
- Von AWS Elastic Load Balancing V2 definierte Ressourcentypen
- Bedingungsschlüssel für AWS Elastic Load Balancing V2

Von AWS Elastic Load Balancing V2 definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den

Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddListenerCertificates	Gewährt die Berechtigung zum Hinzufügen der angegebenen Zertifikate zum angegebenen sicheren Listener.	Schreiben	listener/app*		
			listener/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
AddTags	Gewährt die Berechtigung zum Hinzufügen der angegebenen Tags zum angegebenen Load Balancer. Jeder Load Balancer kann maximal 10 Tags aufweisen.	Markierung	listener-rule/app		
			listener-rule/net		
			listener/app		
			listener/net		
			loadbalancer/app/		
			loadbalancer/net/		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			targetgroup		
			truststore		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:CreateAction	
AddTrustStoreRevocations	Gewährt die Berechtigung zum Hinzufügen von Widerrufen zu einem Trust Store	Schreiben	truststore*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateListener	Gewährt die Berechtigung zum Erstellen eines Listeners für den angegebenen Application Load Balancer.	Schreiben	loadbalancer/app/		elasticloadbalancing:AddTags
			loadbalancer/net/		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy elasticloadbalancing:ListenerProtocol	
CreateLoadBalancer	Gewährt die Berechtigung zum Erstellen eines Load Balancers	Schreiben	loadbalancer/app/		elasticloadbalancing:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			loadbalancer/net/		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup elasticloadbalancing:Subnet elasticloadbalancing:Scheme	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateRule	Gewährt die Berechtigung zum Erstellen einer Regel für den angegebenen Listener.	Schreiben	listener/app*		elasticloadbalancing:AddTags
			listener/net*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateTargetGroup	Gewährt die Berechtigung zum Erstellen einer Zielgruppe	Schreiben	targetgroup*		elasticloadbalancing:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateTrustStore	Gewährt die Berechtigung zum Erstellen eines Vertrauensspeichers	Schreiben	truststore		elasticloadbalancing:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteListener	Gewährt die Berechtigung zum Löschen des angegebenen Listeners.	Schreiben	listener/app*		
			listener/net*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteLoadBalancer	Gewährt die Berechtigung zum Löschen des angegebenen Load Balancers.	Schreiben	loadbalancer/app/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteRule	Gewährt die Berechtigung zum Löschen der angegebenen Regel.	Schreiben	listener-rule/app*		
			listener-rule/net*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteTargetGroup	Gewährt die Berechtigung zum Löschen der angegebenen Zielgruppe.	Schreiben	targetgroup*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteTrustStore	Gewährt die Berechtigung zum Löschen des angegebenen Vertrauensspeichers	Schreiben	truststore*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeregisterTargets	Gewährt die Berechtigung zum Aufheben der Registrierung der angegebenen Ziele in der angegebenen Zielgruppe.	Schreiben	targetgroup*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DescribeAccountLimits	Gewährt die Berechtigung zum Beschreiben der Elastic-Load-Balancing-Ressourcenlimits für das AWS-Konto.	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeListenerCertificates	Gewährt die Berechtigung zum Beschreiben der Zertifikate für den angegebenen sicheren Listener.	Lesen			
DescribeListeners	Gewährt die Berechtigung zum Beschreiben des oder der angegebenen Listener für den angegebenen Application Load Balancer.	Lesen			
DescribeLoadBalancerAttributes	Gewährt die Berechtigung zum Beschreiben der Attribute für den angegebenen Load Balancer.	Lesen			
DescribeLoadBalancers	Gewährt die Berechtigung zum Beschreiben der angegebenen Load Balancer. Wenn keine Load Balancer angegeben werden, beschreibt der Aufruf alle Ihre Load Balancer.	Lesen			
DescribeRules	Gewährt die Berechtigung zum Beschreiben der angegebenen Regel oder der angegebenen Regeln für den angegebenen Listener.	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeSSLPolicies	Gewährt die Berechtigung zum Beschreiben der angegebenen Richtlinie oder aller Richtlinien für die SSL-Aushandlung.	Lesen			
DescribeTags	Gewährt die Berechtigung zum Beschreiben der Tags, die der angegebenen Ressource zugeordnet sind.	Lesen			
DescribeTargetGroupAttributes	Gewährt die Berechtigung zum Beschreiben der Attribute für die angegebene Zielgruppe.	Lesen			
DescribeTargetGroups	Gewährt die Berechtigung zum Beschreiben der angegebenen Zielgruppen oder aller Zielgruppen.	Lesen			
DescribeTargetHealth	Gewährt die Berechtigung zum Beschreiben des Zustands der angegebenen Zielgruppen oder aller Zielgruppen.	Lesen			
DescribeTrustStoreAssociations	Gewährt die Berechtigung zum Beschreiben der Assoziationen mit einem Vertrauensspeicher	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeTrustStoreRevocations	Gewährt die Berechtigung zum Beschreiben der angegebenen Vertrauensspeicher-Widerrufe oder aller Widerrufe im Zusammenhang mit einem Vertrauensspeicher.	Lesen			
DescribeTrustStores	Gewährt die Berechtigung zum Beschreiben der angegebenen Vertrauensspeicher oder aller Vertrauensspeicher	Lesen			
GetTrustStoreCaCertificatesBundle	Gewährt die Berechtigung zum Abrufen eines Vertrauensspeicher-CA-Zertifikatspakets	Lesen	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
GetTrustStoreRevocationContent	Gewährt die Berechtigung zum Abrufen eines Vertrauensspeichers-Widerrufsinhalts	Lesen	truststore*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyListener	Gewährt die Berechtigung zum Ändern der angegebenen Eigenschaften des angegebenen Listeners.	Schreiben	listener/app*		
			listener/net*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy elasticloadbalancing:ListenerProtocol	
ModifyLoadBalancerAttributes	Gewährt die Berechtigung zum Ändern der Attribute für den angegebenen Load Balancer.	Schreiben	loadbalancer/app/ loadbalancer/net/		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyRule	Gewährt die Berechtigung zum Ändern der angegebenen Regel.	Schreiben	listener-rule/app*		
			listener-rule/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyTargetGroup	Gewährt die Berechtigung zum Ändern der Zustandsprüfungen zur Bewertung des Zustands der Ziele in der angegebenen Zielgruppe.	Schreiben	targetgroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyTargetGroupAttributes	Gewährt die Berechtigung zum Ändern der angegebenen Attribute der angegebenen Zielgruppe.	Schreiben	targetgroup*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyTrustStore	Gewährt die Berechtigung zum Ändern des angegebenen Vertrauensspeichers	Schreiben	truststore*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RegisterTargets	Gewährt die Berechtigung zum Registrieren der angegebenen Ziele in der angegebenen Zielgruppe.	Schreiben	targetgroup*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveListenerCertificates	Gewährt die Berechtigung zum Entfernen der angegebenen Zertifikate des angegebenen sicheren Listeners.	Schreiben	listener/app*		
			listener/net*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveTags	Gewährt die Berechtigung zum Entfernen eines oder mehrerer Tags aus dem angegebenen Load Balancer.	Markierung	listener-rule/app		
			listener-rule/net		
			listener/app		
			listener/net		
			loadbalancer/app/		
			loadbalancer/net/		
			targetgroup		
			truststore		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveTrustStoreRevocations	Gewährt die Berechtigung zum Entfernen von Widerrufen aus einem Vertrauensspeicher	Schreiben	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SetIpAddressType	Gewährt die Berechtigung zum Festlegen des Typs der IP-Adressen, die von den Subnetzen des angegebenen Load Balancers verwendet werden.	Schreiben	loadbalancer/app/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetRulePriorities	Gewährt die Berechtigung zum Festlegen der Prioritäten der angegebenen Regeln	Schreiben	listener-rule/app*		
			listener-rule/net*		
SetSecurityGroups	Gewährt die Berechtigung zum Zuordnen der angegebenen Sicherheitsgruppen für den angegebenen Load Balancer.	Schreiben	loadbalancer/app/		
			loadbalancer/net/		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup	
SetSubnets	Gewährt die Berechtigung zum Aktivieren der Availability Zone für die angegebenen Subnetze für den angegebenen Load Balancer.	Schreiben	loadbalancer/app/		
			loadbalancer/net/		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:Subnet	
SetWebAcl [nur Berechtigung]	Gewährt die Berechtigung zum Erteilen einer WebAcl-Berechtigung für WAF.	Schreiben			

Von AWS Elastic Load Balancing V2 definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
listener/app	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener/app/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
listener-rule/app	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener-rule/app/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}/${ListenerRuleId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
listener/net	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener/net/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
listener-rule/net	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener-rule/net/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}/${ListenerRuleId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
loadbalancer/app/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
loadbalancer/net/	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/net/${LoadBalancerName}/${LoadBalancerId}`	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
targetgroup	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:targetgroup/${TargetGroupName}/${TargetGroupId}`	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
truststore	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:truststore/${TrustStoreName}/${TrustStoreId}`	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Elastic Load Balancing V2

AWS Elastic Load Balancing V2 definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wertepaaren, die in der Anforderung zulässig sind	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paar einer Ressource	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach Liste von Tag-Schlüsseln, die in der Anforderung zulässig sind	ArrayOfString
elasticloadbalancing:CreateAction	Filtert den Zugriff nach Name einer ressourcenerstellenden API-Aktion	Zeichenfolge
elasticloadbalancing:ListenerProtocol	Filtert den Zugriff durch das Listener-Protokoll, das in der Anforderung zulässig ist	Zeichenfolge
elasticloadbalancing:ResourceTag/${TagKey}	Filtert den Zugriff nach vorangestellter Zeichenfolge eines Tag-Schlüssel/Wertepaars, das an eine Ressource angefügt ist	Zeichenfolge
elasticloadbalancing:Scheme	Filtert den Zugriff durch das Load-Balancer-Schema, das in der Anforderung zulässig ist	Zeichenfolge
elasticloadbalancing:SecurityGroup	Filtert den Zugriff durch die Sicherheitsgruppen-IDs, die in der Anforderung zulässig sind	ArrayOfString

Bedingungsschlüssel	Beschreibung	Typ
elasticloadbalancing:SecurityPolicy	Filtert den Zugriff durch die SSL-Sicherheitsrichtlinien, die in der Anfrage zulässig sind	ArrayOfString
elasticloadbalancing:Subnet	Filtert den Zugriff durch die Subnetz-IDs, die in der Anfrage zulässig sind	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Elastic MapReduce

Amazon Elastic MapReduce (Servicepräfix: `elasticmapreduce`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Elastic definierte Aktionen MapReduce
- Von Amazon Elastic definierte Ressourcentypen MapReduce
- Bedingungsschlüssel für Amazon Elastic MapReduce

Von Amazon Elastic definierte Aktionen MapReduce

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWSzu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den

Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

> **Note**
>
> Die DescribeJobFlows API ist veraltet und wird schließlich entfernt. Wir empfehlen Ihnen ListClusters, stattdessen DescribeCluster, ListInstanceGroups und ListBootstrapActions zu verwenden ListSteps.

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddInstanceFleet	Gewährt die Berechtigung zum Hinzufügen einer Instance-Flotte zu einem aktiven Cluster	Schreiben	cluster*		
AddInstanceGroups	Gewährt die Berechtigung zum Hinzufügen von Instance-Gruppen zu einem aktiven Cluster	Schreiben	cluster*		
AddJobFlowSteps	Gewährt die Berechtigung zum Hinzufügen neuer Schritte zu einem aktiven Cluster	Schreiben	cluster*		
				elasticmapreduce:ExecutionRoleArn	
AddTags	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Amazon-EMR-Ressource	Tagging	cluster		
			editor		
			notebook-execution		
			studio		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				elasticmapreduce:RequestTag/${TagKey}	
AttachEditor [nur Berechtigung]	Gewährt die Berechtigung zum Anfügen eines EMR-Notebooks an eine Computing-Engine	Schreiben	editor*		
CancelSteps	Gewährt die Berechtigung zum Abbrechen einzelner oder mehrerer Schritte in einem aktiven Cluster	Schreiben	cluster*		
CreateEditor [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines EMR-Notebooks	Schreiben	cluster		
				aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreatePersistentAppUI	Gewährt die Berechtigung zum Erstellen eines persistenten Anwendungsverlaufservers	Schreiben	cluster*		
CreateRepository [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer EMR-Notebook-Repository	Schreiben			
CreateSecurityConfiguration	Gewährt die Berechtigung zum Erstellen einer Sicherheitskonfiguration.	Schreiben			
CreateStudio	Gewährt die Berechtigung zum Erstellen eines EMR-Studios	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
CreateStudioPresignedUrl	Gewährt die Berechtigung zum Starten eines EMR-Studios im IAM-Authentifizierungsmodus	Schreiben	studio*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateStudioSessionMapping	Gewährt die Berechtigung zum Erstellen einer EMR-Studio-Sitzungsmapping	Schreiben	studio*		
DeleteEditor [nur Berechtigung]	Gewährt die Berechtigung zum Löschen eines EMR-Notebooks	Schreiben	editor*		
DeleteRepository [nur Berechtigung]	Gewährt die Berechtigung zum Löschen eines EMR-Notebook-Repositorys	Schreiben			
DeleteSecurityConfiguration	Gewährt die Berechtigung zum Löschen einer Sicherheitskonfiguration.	Schreiben			
DeleteStudio	Gewährt die Berechtigung zum Löschen eines EMR-Studios	Schreiben	studio*		
DeleteStudioSessionMapping	Gewährt die Berechtigung zum Löschen einer EMR-Studio-Sitzungsmapping	Schreiben	studio*		
DeleteWorkspaceAccess [nur Berechtigung]	Erteilt die Berechtigung, eine Identität daran zu hindern, einen kollaborativen WorkSpace zu öffnen	Berechtigungsverwaltung	editor*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeCluster	Gewährt die Berechtigung zum Abrufen von Details über einen Cluster, einschließlich Status, Hardware- und Softwarekonfiguration, VPC-Einstellungen und so weiter	Lesen	cluster*		
DescribeEditor [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen von Informationen zu einem Notebook, einschließlich Status, Benutzer, Rolle, Tags, Speicherort und vieles mehr	Lesen	editor*		
DescribeJobFlows	Gewährt die Berechtigung zum Beschreiben von Details von Clustern (Auftragsabläufe). Diese API ist veraltet und wird letztendlich entfernt werden. Wir empfehlen Ihnen ListClusters, ListBootstrapActions stattdessen DescribeCluster, ListInstanceGroups und zu verwenden ListSteps.	Lesen	cluster*		
DescribeNotebookExecution	Gewährt die Berechtigung zum Anzeigen von Informationen über eine Notebook-Ausführung	Lesen	notebook-execution*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribePersistentAppUI	Gewährt die Berechtigung zum Beschreiben eines persistenten Anwendungsverlaufsservers	Lesen	cluster*		
DescribeReleaseLabel	Gewährt die Berechtigung zum Anzeigen von Informationen über eine EMR-Version, z. B., welche Anwendungen unterstützt werden	Lesen			
DescribeRepository [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben eines EMR-Notebook-Repositorys	Lesen			
DescribeSecurityConfiguration	Gewährt die Berechtigung zum Abrufen von Details einer Sicherheitskonfiguration	Lesen			
DescribeStep	Gewährt die Berechtigung zum Abrufen von Details über einen Cluster-Schritt	Lesen	cluster*		
DescribeStudio	Gewährt die Berechtigung zum Anzeigen von Informationen über ein EMR-Studio	Lesen	studio*		
DetachEditor [nur Berechtigung]	Gewährt die Berechtigung zum Trennen eines EMR-Notebooks von einer Computing-Engine	Schreiben	editor*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAutoTerminationPolicy	Gewährt die Berechtigung zum Abrufen der einem Cluster zugeordneten Richtlinie für die automatische Beendigung	Lesen	cluster*		
GetBlockPublicAccessConfiguration	Gewährt die Berechtigung zum Abrufen der EMR-Block-Konfiguration für den öffentlichen Zugriff für das AWS-Konto in der Region	Lesen			
GetClusterSessionCredentials	Gewährt die Berechtigung zum Abrufen von grundlegenden HTTP-Anmeldeinformationen, die mit einer bestimmten IAM-Ausführungsrolle für einen EMR-Cluster mit differenzierter Zugriffskontrolle verknüpft sind	Schreiben	cluster*		
				elasticmapreduce:ExecutionRoleArn	
GetManagedScalingPolicy	Gewährt die Berechtigung zum Abrufen der verwalteten Skalierungsrichtlinie, die einem Cluster zugeordnet ist	Lesen	cluster*		
GetOnClusterAppUIPresignedURL	Gewährt die Berechtigung zum Abrufen einer vorsignierten URL für einen Anwendungsverlaufsserver, der auf dem Cluster ausgeführt wird	Schreiben	cluster*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetPersistentAppUIPresignedURL	Gewährt die Berechtigung zum Abrufen einer vorsignierten URL für einen persistenten Anwendungsverlaufsserver	Schreiben	cluster*		
GetStudioSessionMapping	Gewährt die Berechtigung zum Anzeigen von Informationen über eine EMR-Sitzungsmapping	Lesen	studio*		
LinkRepository [nur Berechtigung]	Gewährt die Berechtigung zum Verknüpfen eines EMR-Notebook-Repositorys mit EMR-Notebooks	Schreiben			
ListBootstrapActions	Gewährt die Berechtigung zum Abrufen von Details über die Bootstrap-Aktionen, die mit einem Cluster verknüpft sind	Lesen	cluster*		
ListClusters	Gewährt die Berechtigung zum Abrufen des Status zugänglicher Cluster	Auflisten			
ListEditors [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Übersichtsinformationen zugänglicher EMR-Notebooks	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListInstanceFleets	Gewährt die Berechtigung zum Abrufen von Details über die Instance-Flotten in einem Cluster	Lesen	cluster*		
ListInstanceGroups	Gewährt die Berechtigung zum Abrufen von Details über die Instance-Gruppen in einem Cluster	Lesen	cluster*		
ListInstances	Gewährt die Berechtigung zum Abrufen von Details über die Amazon-EC2-Instances in einem Cluster	Lesen	cluster*		
ListNotebookExecutions	Gewährt die Berechtigung zum Auflisten von Übersichtsinformationen für Notebook-Ausführungen	Auflisten			
ListReleaseLabels	Gewährt die Berechtigung zum Auflisten und Filtern der verfügbaren EMR-Versionen in der aktuellen Region	Auflisten			
ListRepositories [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten bestehender EMR-Notebook-Repositorys	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListSecurityConfigurations	Gewährt die Berechtigung zum Auflisten verfügbarer Sicherheitskonfigurationen in diesem Konto nach Namen sowie Datum und Uhrzeit der Erstellung	Auflisten			
ListSteps	Gewährt die Berechtigung zum Auflisten von Schritten, die mit einem Cluster verknüpft sind	Lesen	cluster*		
ListStudioSessionMappings	Gewährt die Berechtigung zum Auflisten zusammenfassender Informationen über EMR-Studio-Sitzungsmappings	Auflisten			
ListStudios	Gewährt die Berechtigung zum Auflisten zusammenfassender Informationen über EMR-Studios	Auflisten			
ListSupportedInstanceTypes	Gewährt die Berechtigung, die Amazon-EC2-Instance-Typen aufzulisten, die von einer Amazon-EMR-Version unterstützt werden	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListWorkspaceAccessIdentities [nur Berechtigung]	Erteilt die Berechtigung zum Auflisten von Identitäten, denen Zugriff auf einen Workspace gewährt wurde	Auflisten	editor*		
ModifyCluster	Gewährt die Berechtigung, Clustereinstellungen zu ändern, wie z. B. die Anzahl der Schritte, die gleichzeitig für einen Cluster ausgeführt werden können	Schreiben	cluster*		
ModifyInstanceFleet	Gewährt die Berechtigung zum Ändern der On-Demand- und Spot-Zielkapazitäten für eine Instance-Flotte	Schreiben	cluster*		
ModifyInstanceGroups	Gewährt die Berechtigung zum Ändern der Anzahl und Konfiguration von EC2-Instances für eine Instance-Gruppe	Schreiben	cluster		
OpenEditorInConsole [nur Berechtigung]	Gewährt die Berechtigung zum Starten des Jupyter-Notebook-Editors für ein EMR-Notebook innerhalb der Konsole	Schreiben	editor* cluster		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutAutoScalingPolicy	Gewährt die Berechtigung zum Erstellen oder Aktualisieren einer Auto-Scaling-Richtlinie für eine Core-Instance-Gruppe oder Aufgabe-Instance-Gruppe.	Schreiben	cluster*		
PutAutoTerminationPolicy	Gewährt die Berechtigung zum Erstellen oder Aktualisieren der einem Cluster zugeordneten Richtlinie für die automatische Beendigung	Schreiben	cluster*		
PutBlockPublicAccessConfiguration	Gewährt die Berechtigung zum Erstellen oder Aktualisieren der EMR-Block-Konfiguration für den öffentlichen Zugriff für das AWS-Konto in der Region	Berechtigungsverwaltung			
PutManagedScalingPolicy	Gewährt die Berechtigung zum Erstellen oder Aktualisieren der verwalteten Skalierungsrichtlinie, die einem Cluster zugeordnet ist	Schreiben	cluster*		
PutWorkspaceAccess [nur Berechtigung]	Erteilt die Berechtigung, einer Identität das Öffnen eines kollaborativen Workspace zu erlauben	Berechtigungsverwaltung	editor*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RemoveAutoScalingPolicy	Gewährt die Berechtigung zum Entfernen einer Auto-Scaling-Richtlinie aus einer Instance-Gruppe.	Schreiben	cluster*		
RemoveAutoTerminationPolicy	Gewährt die Berechtigung zum Entfernen der einem Cluster zugeordneten Richtlinie für die automatische Beendigung	Schreiben	cluster*		
RemoveManagedScalingPolicy	Gewährt die Berechtigung zum Entfernen der verwalteten Skalierungsrichtlinie, die einem Cluster zugeordnet ist	Schreiben	cluster*		
RemoveTags	Gewährt die Berechtigung zum Entfernen von Tags aus einer Amazon-EMR-Ressource.	Tagging	cluster		
			editor		
			notebook-execution		
			studio		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RunJobFlow	Gewährt die Berechtigung zum Erstellen und Starten eines Clusters (Auftragsverlauf)	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	iam:PassRole
SetKeepJobFlowAliveWhenNoSteps	Gewährt die Berechtigung zum Hinzufügen und Entfernen von automatischem Beenden nach der Schrittausführung für einen Cluster	Schreiben	cluster*		
SetTerminationProtection	Gewährt die Berechtigung zum Hinzufügen und Entfernen des Beendigungsschutzes für einen Cluster	Schreiben	cluster*		
SetUnhealthyNodeReplacement	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren des fehlerhaften Knotenaustauschs für einen Cluster	Schreiben	cluster*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SetVisibleToAllUsers	Gewährt die Berechtigung zum Festlegen, ob alle AWS Identity and Access Management (IAM)-Benutzer in der einen Cluster anzeigen AWS-Konto können. Diese API ist veraltet und Ihr Cluster ist möglicherweise für alle Benutzer in Ihrem Konto sichtbar. Informationen zum Einschränken des Clusterzugriffs mithilfe einer IAM-Richtlinie finden Sie unter AWS Identity and Access Management für Amazon EMR (https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-plan-access-iam.html)	Schreiben	cluster*		
StartEditor [nur Berechtigung]	Gewährt die Berechtigung zum Starten eines EMR-Notebooks	Schreiben	editor* cluster		
StartNotebookExecution	Gewährt die Berechtigung zum Starten einer EMR-Notebook-Ausführung	Schreiben	cluster* editor*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
StopEditor [nur Berechtigung]	Gewährt die Berechtigung zum Schließen eines EMR-Notebooks	Schreiben	editor*		
StopNotebookExecution	Gewährt die Berechtigung zum Beenden der Notebook-Ausführung	Schreiben	notebook-execution*		
TerminateJobFlows	Gewährt die Berechtigung zum Beenden eines Clusters (Auftragsverlauf)	Schreiben	cluster*		
UnlinkRepository [nur Berechtigung]	Gewährt die Berechtigung zum Aufheben eines EMR Notebook-Repositorys von EMR-Notebooks	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateEditor [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren eines EMR-Notebook	Schreiben	editor*		
UpdateRepository [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren eines EMR-Notebook-Repositorys	Schreiben			
UpdateStudio	Gewährt die Berechtigung zum Aktualisieren von Informationen über ein EMR-Studio	Schreiben	studio*		
UpdateStudioSessionMapping	Gewährt die Berechtigung zum Aktualisieren einer EMR-Studio-Sitzungsmapping	Schreiben	studio*		
ViewEventsFromAllClustersInConsole [nur Berechtigung]	Gewährt die Berechtigung zum Verwenden der EMR-Konsole, um Ereignisse aus allen Clustern anzuzeigen	Auflisten			

Von Amazon Elastic definierte Ressourcentypen MapReduce

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
cluster	`arn:${Partition}:elasticmapreduce:${Region}:${Account}:cluster/${ClusterId}`	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}
editor	`arn:${Partition}:elasticmapreduce:${Region}:${Account}:editor/${EditorId}`	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}
notebook-execution	`arn:${Partition}:elasticmapreduce:${Region}:${Account}:notebook-execution/${NotebookExecutionId}`	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}
studio	`arn:${Partition}:elasticmapreduce:${Region}:${Account}:studio/${StudioId}`	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Elastic MapReduce

Amazon Elastic MapReduce definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend darauf, ob das Tag-Wert-Paar mit der Aktion bereitgestellt wird.	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf dem Tag-Wert-Paar, das einer Amazon-EMR-Ressource zugeordnet ist.	String
aws:TagKeys	Filtert den Zugriff basierend darauf, ob die Tag-Schlüssel mit der Aktion bereitgestellt werden, unabhängig vom Tag-Wert.	ArrayOfString
elasticmapreduce:ExecutionRoleArn	Filtert den Zugriff danach, ob die ARN der Ausführungsrolle mit der Aktion bereitgestellt wird	ARN
elasticmapreduce:RequestTag/${TagKey}	Filtert den Zugriff basierend darauf, ob das Tag-Wert-Paar mit der Aktion bereitgestellt wird.	String
elasticmapreduce:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf dem Tag-Wert-Paar, das einer Amazon-EMR-Ressource zugeordnet ist.	String

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Elastic Transcoder

Amazon Elastic Transcoder (Servicepräfix: `elastictranscoder`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Elastic Transcoder definierte Aktionen
- Von Amazon Elastic Transcoder definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Elastic Transcoder

Von Amazon Elastic Transcoder definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelJob	Auftrag abbrechen, mit dessen Verarbeitung Elastic Transcoder noch nicht begonnen hat	Schreiben	job*		
CreateJob	Erstellen eines Auftrags	Schreiben	pipeline*		
			preset*		
CreatePipeline	Erstellen Sie eine Pipeline	Schreiben			
CreatePreset	Voreinstellung erstellen	Schreiben			
DeletePipeline	Pipeline löschen	Write	pipeline*		
DeletePreset	Voreinstellung löschen	Write	preset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListJobsByPipeline	Liste der Aufträge abrufen, die Sie einer Pipeline zugewiesen haben	List	pipeline*		
ListJobsByStatus	Informationen zu allen Aufträgen abrufen, die dem aktuellen AWS-Konto zugeordnet sind und den angegebenen Status aufweisen	List			
ListPipelines	Liste der Pipelines abrufen, die dem aktuellen AWS-Konto zugeordnet sind	Auflisten			
ListPresets	Liste aller Voreinstellungen abrufen, die dem aktuellen AWS-Konto zugeordnet sind	Auflisten			
ReadJob	Detaillierte Informationen zu einem Auftrag abrufen	Read	job*		
ReadPipeline	Detaillierte Informationen zu einer Pipeline abrufen	Lesen	pipeline*		
ReadPreset	Detaillierte Informationen zu einer Voreinstellung abrufen	Lesen	preset*		
TestRole	Einstellungen für eine Pipeline testen und sicherstellen, dass Elastic Transcoder Aufträge erstellen und verarbeiten kann	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdatePipeline	Einstellungen für eine Pipeline aktualisieren	Write	pipeline*		
UpdatePipelineNotifications	Nur Amazon Simple Notification Service (Amazon SNS)-Benachrichtigungen für eine Pipeline aktualisieren	Schreiben	pipeline*		
UpdatePipelineStatus	Pipeline anhalten oder reaktivieren, damit die Pipeline die Verarbeitung von Aufträgen stoppt bzw. fortsetzt; Status der Pipeline aktualisieren	Schreiben	pipeline*		

Von Amazon Elastic Transcoder definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
job	`arn:${Partition}:elastictranscoder:${Region}:${Account}:job/${JobId}`	

Ressource ntypen	ARN	Bedingungsschlüssel
pipeline	`arn:${Partition}:elastictranscoder:${Region}:${Account}:pipeline/${PipelineId}`	
preset	`arn:${Partition}:elastictranscoder:${Region}:${Account}:preset/${PresetId}`	

Bedingungsschlüssel für Amazon Elastic Transcoder

Elastic Transcoder besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon ElastiCache

Amazon ElastiCache (Servicepräfix: `elasticache`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon definierte Aktionen ElastiCache
- Von Amazon definierte Ressourcentypen ElastiCache
- Bedingungsschlüssel für Amazon ElastiCache

Von Amazon definierte Aktionen ElastiCache

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWSzu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

> **Note**
>
> Wenn Sie eine - ElastiCache Richtlinie in IAM erstellen, müssen Sie das Platzhalterzeichen „*“ für den Ressourcenblock verwenden. Informationen zur Verwendung der folgenden ElastiCache API-Aktionen in einer IAM-Richtlinie finden Sie unter ElastiCache Aktionen und IAM im Amazon- ElastiCache Benutzerhandbuch.

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddTagsToResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer - ElastiCache Ressource	Tagging	cluster		
			parametergroup		
			replicationgroup		
			reserved-instance		
			securitygroup		
			serverlesscache		
			serverlesscachesnapshot		
			snapshot		
			subnetgroup		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			user		
			usergroup		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
AuthorizeCacheSecurityGroupIngress	Gewährt die Berechtigung zum Autorisieren einer EC2-Sicherheitsgruppe für eine ElastiCache Sicherheitsgruppe	Schreiben	securitygroup*		ec2:AuthorizeSecurityGroupIngress
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchApplyUpdateAction	Gewährt die Berechtigung zum Anwenden von ElastiCache Service-Updates auf Cluster und Replikationsgruppen	Schreiben	cluster		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs s3:GetObject
			replicationgroup		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchStopUpdateAction	Gewährt die Berechtigung zum Beenden der Ausführung von ElastiCache Service-Updates auf einer Gruppe von Clustern	Schreiben	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
CompleteMigration	Gewährt die Berechtigung zum Abschließen einer Online-Migration von Daten von gehostetem Redis auf Amazon EC2 zu ElastiCache	Schreiben	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
Connect	Gewährt die Berechtigung zum Herstellen einer Verbindung als angegebener ElastiCache Benutzer mit einer ElastiCache -Replikationsgruppe oder einem ElastiCache Serverless-Cache	Schreiben	user*		
			replicationgroup		
			serverlesscache		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CopyServerlessCacheSnapshot	Gewährt die Berechtigung zum Erstellen einer Kopie eines vorhandenen Serverless-Cache-Snapshots	Schreiben	serverlesscachesnapshot*	aws:ResourceTag/${TagKey} elasticache:KmsKeyId	elasticache:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CopySnapshot	Gewährt die Berechtigung zum Erstellen einer Kopie eines vorhandenen Snapshots	Write	snapshot*		elasticache:AddTagsToResource s3:DeleteObject s3:GetBucketAcl s3:PutObject

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys elasticache:KmsKeyId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCacheCluster	Gewährt die Berechtigung zum Erstellen eines Cache-Clusters	Write	parametergroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs elasticache:AddTagsToResource s3:GetObject

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			cluster	aws:RequestTag/${TagKey} aws:TagKeys elasticache:CacheNodeType elasticache:EngineVersion elasticache:EngineType elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				elasticache:CacheParameterGroupName	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			replicationgroup	elasticache:CacheNodeType elasticache:EngineVersion elasticache:EngineType elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:CacheParameterGroupName	
			securitygroup		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			snapshot		
			subnetgroup		
				aws:ResourceTag/${TagKey}	
CreateCacheParameterGroup	Gewährt die Berechtigung zum Erstellen einer Parametergruppe	Write	parametergroup*		elasticache:AddTagsToResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys elasticache:CacheParameterGroupName	
CreateCacheSecurityGroup	Gewährt die Berechtigung zum Erstellen einer Cache-Sicherheitsgruppe	Write	securitygroup*		elasticache:AddTagsToResource

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateCacheSubnetGroup	Gewährt die Berechtigung zum Erstellen einer Cache-Subnetzgruppe	Write	subnetgroup*		elasticache:AddTagsToResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateGlobalReplicationGroup	Gewährt die Berechtigung zum Erstellen einer globalen Replikationsgruppe	Write	globalreplicationgroup*		
			replicationgroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
CreateReplicationGroup	Gewährt die Berechtigung zum Erstellen einer Replikationsgruppe	Schreiben	parametergroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs elasticache:AddTagsToResource s3:GetObject
			cluster		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			globalreplicationgroup	elasticache:NumNodeGroups elasticache:CacheNodeType elasticache:ReplicasPerNodeGroup elasticache:EngineVersion elasticache:EngineType elasticache:AtRestEncryptionEnabled elasticache:TransitEncryptionEnabled elasticache:AutomaticFailov	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				erEnabled elasticache:MultiAZEnabled elasticache:ClusterModeEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:KmsKeyId elasticache:CacheParameterGroupName	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			replicationgroup	aws:RequestTag/${TagKey} aws:TagKeys elasticache:NumNodeGroups elasticache:CacheNodeType elasticache:ReplicasPerNodeGroup elasticache:EngineVersion elasticache:EngineType elasticache:AtRestEncryptionEnabled	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				elasticache:TransitEncryptionEnabled elasticache:AutomaticFailoverEnabled elasticache:MultiAZEnabled elasticache:ClusterModeEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:KmsKeyId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				elasticache:CacheParameterGroupName	
			securitygroup		
			snapshot		
			subnetgroup		
			usergroup		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateServerlessCache	Gewährt die Berechtigung zum Erstellen eines Serverless-Cache	Schreiben	serverlesscache*	aws:ResourceTag/${TagKey} elasticache:EngineType elasticache:EngineVersion elasticache:SnapshotRetentionLimit elasticache:KmsKeyId elasticache:MaximumDataStorage elasticache:DataStorageUnit elasticache:MaximumECPUPerSecond	ec2:CreateTags ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeTags ec2:DescribeVpcEndpoints ec2:DescribeVpcs elasticache:AddTagsToResource

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					s3:GetObject
			serverlesscachesnapshot	aws:ResourceTag/${TagKey}	
			snapshot	aws:ResourceTag/${TagKey}	
			usergroup	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateServerlessCacheSnapshot	Gewährt die Berechtigung zum Erstellen einer Kopie eines Serverless-Cache zu einem bestimmten Zeitpunkt	Schreiben	serverlesscache*	aws:ResourceTag/${TagKey}	elasticache:AddTagsToResource
			serverlesscachesnapshot*	aws:ResourceTag/${TagKey} elasticache:KmsKeyId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshot	Gewährt die Berechtigung zum Erstellen einer Kopie eines gesamten Redis-Clusters zu einem bestimmten Zeitpunkt	Schreiben	snapshot*	aws:RequestTag/${TagKey} aws:TagKeys elasticache:KmsKeyId	elasticache:AddTagsToResource s3:DeleteObject s3:GetBucketAcl s3:PutObject
			cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
CreateUser	Gewährt die Berechtigung zum Erstellen eines Benutzers für Redis. Benutzer werden ab Redis 6.0 unterstützt	Schreiben	user*		elasticache:AddTagsToResource

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys elasticache:UserAuthenticationMode	
CreateUserGroup	Gewährt die Berechtigung zum Erstellen einer Benutzergruppe für Redis. Gruppen werden ab Redis 6.0 unterstützt	Schreiben	user*		elasticache:AddTagsToResource
			usergroup*	aws:RequestTag/${TagKey} aws:TagKeys	
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DecreaseNodeGroupsInGlobalReplicationGroup	Gewährt die Berechtigung zum Verringern der Anzahl der Knotengruppen in globalen Replikationsgruppen	Write	globalreplicationgroup*		
				elasticache:NumNodeGroups	
DecreaseReplicaCount	Gewährt die Berechtigung zum Verringern der Anzahl der Replikate in einer Redis-Replikationsgruppe (Cluster-Modus deaktiviert) oder der Anzahl der Replikationsknoten in einer oder mehreren Knotengruppen (Shards) einer Replikationsgruppe für den Redis-Modus (Clustermodus aktiviert)	Write	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} elasticache:ReplicasPerNodeGroup	
DeleteCacheCluster	Gewährt die Berechtigung zum Löschen eines zuvor bereitgestellten Clusters	Write	cluster*	aws:ResourceTag/${TagKey}	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			snapshot		
DeleteCacheParameterGroup	Gewährt die Berechtigung zum Löschen der angegebenen Cache-Parametergruppe	Write	parametergroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} elasticache:CacheParameterGroupName	
DeleteCacheSecurityGroup	Gewährt die Berechtigung zum Löschen einer Cache-Sicherheitsgruppe	Write	securitygroup*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteCacheSubnetGroup	Gewährt die Berechtigung zum Löschen einer Cache-Subnetzgruppe	Write	subnetgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	
DeleteGlobalReplicationGroup	Gewährt die Berechtigung zum Löschen einer bestehenden globalen Replikationsgruppe	Write	globalreplicationgroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteReplicationGroup	Gewährt die Berechtigung zum Löschen einer vorhandenen Replikationsgruppe	Schreiben	replicationgroup*	aws:ResourceTag/${TagKey}	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			snapshot		
DeleteServerlessCache	Gewährt die Berechtigung zum Löschen eines Serverless-Cache	Schreiben	serverlesscache*	aws:ResourceTag/${TagKey}	ec2:DescribeTags
			serverlesscachesnapshot		
DeleteServerlessCacheSnapshot	Gewährt die Berechtigung zum Löschen eines Serverless-Cache-Snapshots	Schreiben	serverlesscachesnapshot*	aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteSnapshot	Gewährt die Berechtigung zum Löschen eines bestehenden Snapshots	Write	snapshot*		
				aws:ResourceTag/${TagKey}	
DeleteUser	Gewährt die Berechtigung zum Löschen eines vorhandenen Benutzers, um ihn so aus allen Benutzergruppen und Replikationsgruppen zu entfernen, denen er zugewiesen wurde	Write	user*		
				aws:ResourceTag/${TagKey}	
DeleteUserGroup	Gewährt die Berechtigung zum Löschen einer bestehenden Benutzergruppe	Write	usergroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheClusters	Gewährt die Berechtigung zum Auflisten von Informationen über bereitgestellte Cache-Cluster	Auflisten	cluster*		
				aws:ResourceTag/${TagKey}	
DescribeCacheEngineVersions	Gewährt die Berechtigung zum Listen der verfügbaren Cache-Engines und deren Versionen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeCacheParameterGroups	Gewährt die Berechtigung zum Auflisten von Cache-Parametergruppenbeschreibungen	List	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheParameters	Gewährt die Berechtigung zum Zurückgeben der detaillierten Parameterliste für eine bestimmte Cache-Parametergruppe	List	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheSecurityGroups	Gewährt die Berechtigung zum Auflisten von Cache-Sicherheitsgruppenbeschreibungen	List	securitygroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheSubnetGroups	Gewährt die Berechtigung zum Auflisten von Cache-Subnet-Gruppenbeschreibungen	List	subnetgroup*		
				aws:ResourceTag/${TagKey}	
DescribeEngineDefaultParameters	Gewährt die Berechtigung zum Zurückgeben der Standard-Engine- und System-Parameterinformationen für die angegebene Datenbank-Engine	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeEvents	Gewährt die Berechtigung zum Auflisten von Ereignissen im Zusammenhang mit Clustern, Cache-Sicherheitsgruppen und Cache-Parametergruppen	List			
DescribeGlobalReplicationGroups	Gewährt die Berechtigung zum Auflisten von Informationen über globale Replikationsgruppen	List	globalreplicationgroup*		
DescribeReplicationGroups	Gewährt die Berechtigung zum Auflisten von Informationen über bereitgestellte Replikationsgruppen	List	replicationgroup*		
				aws:ResourceTag/${TagKey}	
DescribeReservedCacheNodes	Gewährt die Berechtigung zum Auflisten von Informationen über gekaufte reservierte Cache-Knoten	List	reserved-instance*		
				aws:ResourceTag/${TagKey}	
DescribeReservedCacheNodesOfferings	Gewährt die Berechtigung zum Auflisten verfügbarer reservierter Cache-Knotenangebote	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeServerlessCacheSnapshots	Gewährt die Berechtigung zum Auflisten von Informationen über Serverless-Cache-Snapshots	Auflisten	serverlesscachesnapshot*	aws:ResourceTag/${TagKey}	
			serverlesscache	aws:ResourceTag/${TagKey}	
DescribeServerlessCaches	Gewährt die Berechtigung zum Auflisten von Serverless-Caches	Auflisten	serverlesscache*	aws:ResourceTag/${TagKey}	
DescribeServiceUpdates	Gewährt die Berechtigung zum Auflisten von Details der Service-Updates	List			
DescribeSnapshots	Gewährt die Berechtigung zum Auflisten von Informationen über Snapshots von Clustern oder Replikationsgruppen	List	snapshot*		
				aws:ResourceTag/${TagKey}	
DescribeUpdateActions	Gewährt die Berechtigung zum Auflisten von Details der Aktualisierungsaktionen für eine Reihe von Clustern oder Replikationsgruppen	List	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeUserGroups	Gewährt die Berechtigung zum Auflisten von Informationen über Redis-Benutzergruppen	List	usergroup*		
				aws:ResourceTag/${TagKey}	
DescribeUsers	Gewährt die Berechtigung zum Auflisten von Informationen über Redis-Benutzer	List	user*		
				aws:ResourceTag/${TagKey}	
DisassociateGlobalReplicationGroup	Gewährt die Berechtigung zum Entfernen einer sekundären Replikationsgruppe aus der globalen Replikationsgruppe	Schreiben	globalreplicationgroup*		
ExportServerlessCacheSnapshot	Gewährt die Berechtigung zum Exportieren einer Kopie eines Serverless-Cache zu einem bestimmten Zeitpunkt in ein S3-Bucket	Schreiben	serverlesscachesnapshot*	aws:ResourceTag/${TagKey}	s3:DeleteObject s3:ListAllMyBuckets s3:PutObject
FailoverGlobalReplicationGroup	Gewährt die Berechtigung zum Failover der primären Region auf eine ausgewählte sekundäre Region einer globalen Replikationsgruppe	Write	globalreplicationgroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
IncreaseNodeGroupsInGlobalReplicationGroup	Gewährt die Berechtigung zum Erhöhen der Anzahl der Knotengruppen in einer globalen Replikationsgruppe	Write	globalreplicationgroup*		
				elasticache:NumNodeGroups	
IncreaseReplicaCount	Gewährt die Berechtigung zum Erhöhen der Anzahl der Replikate in einer Redis-Replikationsgruppe (Cluster-Modus deaktiviert) oder der Anzahl der Replikationsknoten in einer oder mehreren Knotengruppen (Shards) einer Replikationsgruppe für den Redis-Modus (Clustermodus aktiviert)	Schreiben	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} elasticache:ReplicasPerNodeGroup	
InterruptClusterAzPower [nur Berechtigung]	Gewährt die Berechtigung zum Testen einer AZ-Leistungsunterbrechung für eine - ElastiCache Ressource	Schreiben	replicationgroup*		
				aws:ResourceTag/${TagKey}	
ListAllowedNodeTypeModifications	Gewährt die Berechtigung zum Auflisten verfügbarer Knotentypen, die zum Skalieren eines bestimmten Redis-Clusters oder einer Replikationsgruppe verwendet werden können	Auflisten	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine - ElastiCache Ressource	Lesen	cluster		
			parametergroup		
			replicationgroup		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			reserved-instance		
			securitygroup		
			serverlesscache		
			serverlesscachesnapshot		
			snapshot		
			subnetgroup		
			user		
			usergroup		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyCacheCluster	Gewährt die Berechtigung zum Ändern von Einstellungen für einen Cluster	Write	cluster*	elasticache:CacheNodeType elasticache:EngineVersion elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:CacheParameterGroupName	
			parametergroup		
			securitygroup		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
ModifyCacheParameterGroup	Gewährt die Berechtigung zum Ändern der Parameter einer Cache-Parametergruppe	Write	parametergroup*		
				aws:ResourceTag/${TagKey} elasticache:CacheParameterGroupName	
ModifyCacheSubnetGroup	Gewährt die Berechtigung zum Ändern einer vorhandenen Cache-Subnetzgruppe	Write	subnetgroup*		
				aws:ResourceTag/${TagKey}	
ModifyGlobalReplicationGroup	Gewährt die Berechtigung zum Ändern von Einstellungen für eine globale Replikationsgruppe	Write	globalreplicationgroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				elasticache:CacheNodeType elasticache:EngineVersion elasticache:AutomaticFailoverEnabled	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyReplicationGroup	Gewährt die Berechtigung zum Ändern der Einstellungen für eine Replikationsgruppe	Write	replicationgroup*	elasticache:CacheNodeType elasticache:EngineVersion elasticache:AutomaticFailoverEnabled elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:CacheParameterGroupName elasticache:Transi	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				tEncryptionEnabled elasticache:ClusterModeEnabled	
			parametergroup		
			securitygroup		
			usergroup		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyReplicationGroupShardConfiguration	Gewährt die Berechtigung zum Hinzufügen von Shards, zum Entfernen von Shards oder zum Ausgleich der Keyspaces unter vorhandenen Shards einer Replikationsgruppe	Schreiben	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey} elasticache:NumNodeGroups	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyServerlessCache	Gewährt die Berechtigung zum Ändern der Parameter eines Serverless-Cache	Schreiben	serverlesscache*	aws:ResourceTag/${TagKey} elasticache:EngineVersion elasticache:SnapshotRetentionLimit elasticache:MaximumDataStorage elasticache:DataStorageUnit elasticache:MaximumECPUPerSecond	ec2:DescribeSecurityGroups ec2:DescribeTags
			usergroup	aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyUser	Gewährt die Berechtigung zum Ändern des Redis-Benutzerpassworts und/oder der Zugriffszeichenfolge	Write	user*		
				aws:ResourceTag/${TagKey} elasticache:UserAuthenticationMode	
ModifyUserGroup	Gewährt die Berechtigung zum Ändern der Liste der Benutzer, die zur Benutzergruppe gehören	Write	user*		
			usergroup*		
				aws:ResourceTag/${TagKey}	
PurchaseReservedCacheNodesOffering	Gewährt die Berechtigung zum Kauf eines Reserved Cache-Knotenangebots	Write	reserved-instance*		elasticache:AddTagsToResource

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
RebalanceSlotsInGlobalReplicationGroup	Gewährt die Berechtigung zum Durchführen eines Keyspace-Rebalance-Vorgangs, um Slots neu zu verteilen und eine einheitliche Schlüsselverteilung über vorhandene Shards in einer globalen Replikationsgruppe sicherzustellen	Write	globalreplicationgroup*		
RebootCacheCluster	Gewährt die Berechtigung zum Neustarten einiger oder aller Cache-Knoten innerhalb eines bereitgestellten Cache-Clusters oder einer Replikationsgruppe (Cluster-Modus deaktiviert)	Schreiben	cluster*		
				aws:ResourceTag/${TagKey}	
RemoveTagsFromResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer ElastiCache Ressource	Tagging	cluster		
			parametergroup		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			replicationgroup		
			reserved-instance		
			securitygroup		
			serverlesscache		
			serverlesscachesnapshot		
			snapshot		
			subnetgroup		
			user		
			usergroup		
				aws:TagKeys aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ResetCacheParameterGroup	Gewährt die Berechtigung, Parameter einer Cache-Parametergruppe wieder auf ihre Standardwerte zu ändern	Schreiben	parametergroup*		
				aws:ResourceTag/${TagKey} elasticache:CacheParameterGroupName	
RevokeCacheSecurityGroupIngress	Gewährt die Berechtigung zum Entfernen eines EC2-Sicherheitsgruppeneingangs aus einer ElastiCache Sicherheitsgruppe	Schreiben	securitygroup*		
				aws:ResourceTag/${TagKey}	
StartMigration	Gewährt die Berechtigung zum Starten einer Migration von Daten von gehostetem Redis auf Amazon EC2 zu ElastiCache für Redis	Schreiben	replicationgroup*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TestFailover	Gewährt die Berechtigung zum Testen des automatischen Failovers für eine bestimmte Knotengruppe in einer Replikationsgruppe	Schreiben	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	
TestMigration	Gewährt die Berechtigung zum Testen einer Migration von Daten von gehostetem Redis auf Amazon EC2 zu ElastiCache für Redis	Schreiben	replicationgroup*		
				aws:ResourceTag/${TagKey}	

Von Amazon definierte Ressourcentypen ElastiCache

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
parametergroup	`arn:${Partition}:elasticache:${Region}:${Account}:parametergroup:${CacheParameterGroupName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:CacheParameterGroupName
securitygroup	`arn:${Partition}:elasticache:${Region}:${Account}:securitygroup:${CacheSecurityGroupName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
subnetgroup	`arn:${Partition}:elasticache:${Region}:${Account}:subnetgroup:${CacheSubnetGroupName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Ressourcentypen	ARN	Bedingungsschlüssel
replicationgroup	`arn:${Partition}:elasticache:${Region}:${Account}:replicationgroup:${ReplicationGroupId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:AtRestEncryptionEnabled elasticache:AuthTokenEnabled elasticache:AutomaticFailoverEnabled elasticache:CacheNodeType elasticache:CacheParameterGroupName elasticache:ClusterModeEnabled elasticache:EngineType elasticache:EngineVersion elasticache:KmsKeyId elasticache:MultiAZEnabled

Ressourcentypen	ARN	Bedingungsschlüssel
		elasticache:NumNodeGroups elasticache:ReplicasPerNodeGroup elasticache:SnapshotRetentionLimit elasticache:TransitEncryptionEnabled

Ressourcentypen	ARN	Bedingungsschlüssel
cluster	arn:${Partition}:elasticache:${Region}:${Account}:cluster:${CacheClusterId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:AuthTokenEnabled elasticache:CacheNodeType elasticache:CacheParameterGroupName elasticache:EngineType elasticache:EngineVersion elasticache:MultiAZEnabled elasticache:SnapshotRetentionLimit
reserved-instance	arn:${Partition}:elasticache:${Region}:${Account}:reserved-instance:${ReservedCacheNodeId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Ressourcentypen	ARN	Bedingungsschlüssel
snapshot	`arn:${Partition}:elasticache:${Region}:${Account}:snapshot:${SnapshotName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:KmsKeyId

Ressourcentypen	ARN	Bedingungsschlüssel
globalreplicationgroup	`arn:${Partition}:elasticache::${Account}:globalreplicationgroup:${GlobalReplicationGroupId}`	elasticache:AtRestEncryptionEnabled elasticache:AuthTokenEnabled elasticache:AutomaticFailoverEnabled elasticache:CacheNodeType elasticache:CacheParameterGroupName elasticache:ClusterModeEnabled elasticache:EngineType elasticache:EngineVersion elasticache:KmsKeyId elasticache:MultiAZEnabled elasticache:NumNodeGroups elasticache:ReplicasPerNodeGroup elasticache:SnapshotRetentionLimit

Ressourcentypen	ARN	Bedingungsschlüssel
		elasticache:TransitEncryptionEnabled
user	arn:${Partition}:elasticache:${Region}:${Account}:user:${UserId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:UserAuthenticationMode
usergroup	arn:${Partition}:elasticache:${Region}:${Account}:usergroup:${UserGroupId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Ressourcentypen	ARN	Bedingungsschlüssel
serverlesscache	arn:${Partition}:elasticache:${Region}:${Account}:serverlesscache:${ServerlessCacheName}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:DataStorageUnit elasticache:EngineType elasticache:EngineVersion elasticache:KmsKeyId elasticache:MaximumDataStorage elasticache:MaximumECPUPerSecond elasticache:SnapshotRetentionLimit
serverlesscachesnapshot	arn:${Partition}:elasticache:${Region}:${Account}:serverlesscachesnapshot:${ServerlessCacheSnapshotName}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:KmsKeyId

Bedingungsschlüssel für Amazon ElastiCache

Amazon ElastiCache definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

> **Note**
>
> Informationen zu Bedingungen in einer IAM-Richtlinie zur Steuerung des Zugriffs auf ElastiCachefinden Sie unter ElastiCache Schlüssel im Amazon- ElastiCache Benutzerhandbuch.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf den Markierungen, die in der Anforderung übergeben werden.	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf den Markierungen, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert Aktionen basierend auf den Tag-Schlüsseln, die in der Anforderung übergeben werden.	ArrayOfString
elasticache:AtRestEncryptionEnabled	Filtert den Zugriff nach dem AtRestEncryptionEnabled Parameter, der in der Anforderung vorhanden ist, oder nach dem Standardwert „false“, wenn der Parameter nicht vorhanden ist	Bool
elasticache:AuthTokenEnabled	Filtert den Zugriff nach dem Vorhandensein eines nicht leeren AuthToken Parameters in der Anforderung	Bool

Bedingungsschlüssel	Beschreibung	Typ
elasticache:AutomaticFailoverEnabled	Filtert den Zugriff nach dem - AutomaticFailoverEnabled Parameter in der Anforderung	Bool
elasticache:CacheNodeType	Filtert den Zugriff nach dem cacheNodeType Parameter, der in der Anforderung vorhanden ist. Mit diesem Schlüssel kann eingeschränkt werden, welche Cache-Knotentypen bei der Clustererstellung oder Skalierung verwendet werden können	String
elasticache:CacheParameterGroupName	Filtert den Zugriff nach dem - CacheParameterGroupName Parameter in der Anforderung	String
elasticache:ClusterModeEnabled	Filtert den Zugriff nach dem in der Anforderung vorhandenen Clustermodus-Parameter. Der Standardwert für Einzelknotengruppen (Shard)-Kreationen ist falsch	Bool
elasticache:DataStorageUnit	Filtert den Zugriff nach CacheUsageLimits.DataStorageEinheitenparameter in der - CreateServerlessCache und - ModifyServerlessCache Anforderung	String
elasticache:EngineType	Filtert den Zugriff nach dem in Erstellungsanforderungen vorhandenen Engine-Typ. Für die Erstellung von Replikationsgruppen wird die Standard-Engine „redis“ als Schlüssel verwendet, wenn der Parameter nicht vorhanden ist	String
elasticache:EngineVersion	Filtert den Zugriff nach dem in Erstellungs- oder Clusteränderungsanforderungen vorhandenen Parameter engineVersion	String

Bedingungsschlüssel	Beschreibung	Typ
elasticache:KmsKeyId	Filtert den Zugriff nach dem - KmsKeyId Parameter in der Anforderung	String
elasticache:MaximumDataStorage	Filtert den Zugriff nach CacheUsageLimits.DataStorageMaximaler Parameter in der - CreateServerlessCache und - ModifyServerlessCache Anforderung	Numerischer Wert
elasticache:MaximumECPUPerSecond	Filtert den Zugriff nach dem Parameter CacheUsageLimits.ECPU PerSecond.Maximum in der - CreateServerlessCache und - ModifyServerlessCache Anforderung	Numerischer Wert
elasticache:MultiAZEnabled	Filtert den Zugriff nach dem AZMode-Parameter, dem MultiAZEnabled-Parameter oder der Anzahl der Availability Zones, in die der Cluster oder die Replikationsgruppe platziert werden kann	Bool
elasticache:NumNodeGroups	Filtert den Zugriff nach dem in der Anforderung angegebenen NodeGroupCount Parameter NumNodeGroups oder . Dieser Schlüssel kann verwendet werden, um die Anzahl der Knotengruppen (Shards) zu beschränken, die Cluster nach Erstellungs- oder SkalierungsProduktionen haben können	Numerischer Wert
elasticache:ReplicasPerNodeGroup	Filtert den Zugriff nach der Anzahl der Replikate pro Knotengruppe (Shards), die in Erstellungs- oder Skalierungsanforderungen angegeben ist	Numerischer Wert
elasticache:SnapshotRetentionLimit	Filtert den Zugriff nach dem - SnapshotRetentionLimit Parameter in der Anforderung	Numerischer Wert

Bedingungsschlüssel	Beschreibung	Typ
elasticache:TransitEncryptionEnabled	Filtert den Zugriff nach dem TransitEncryptionEnabled Parameter, der in der Anforderung vorhanden ist. Für die Erstellung von Replikationsgruppen wird der Standardwert „false“ als Schlüssel verwendet, wenn der Parameter nicht vorhanden ist	Bool
elasticache:UserAuthenticationMode	Filtert den Zugriff nach dem - UserAuthenticationMode Parameter in der Anforderung	String

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elemental Appliances and Software

AWS Elemental Appliances and Software (Servicepräfix: `elemental-appliances-software`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Elemental Appliances and Software definierte Aktionen
- Von AWS Elemental Appliances and Software definierte Ressourcen
- Bedingungsschlüssel für AWS Elemental Appliances and Software

Von AWS Elemental Appliances and Software definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWSzu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CompleteUpload [nur Berechtigung]	Gewährt die Berechtigung zum Abschließen eines Hochladens eines Anhangs für ein Angebot oder eine Bestellung	Schreiben			
CreateOrderV1 [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines Auftrags	Schreiben			
CreateQuote [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines Angebots	Tagging	quote*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetAvsCorrectAddress [nur Berechtigung]	Gewährt die Berechtigung zum Validieren einer Adresse	Lesen			
GetBillingAddresses [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der Rechnungsadressen im AWS Konto	Lesen			
GetDeliveryAddressesV2 [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der Lieferadressen im AWS Konto	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetOrder [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben einer Bestellung	Lesen			
GetOrdersV2 [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der Bestellungen im AWS Konto	Lesen			
GetQuote [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben einer Angebots	Lesen	quote*		
GetTaxes [nur Berechtigung]	Gewährt die Berechtigung zum Berechnen von Steuern für eine Bestellung	Lesen			
ListQuotes [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der Anführungszeichen im AWS Konto	Auflisten			
ListTagsForResource [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Tags für eine - AWS Elemental-Appliances-and-Software-Ressource	Lesen	quote		
StartUpload [nur Berechtigung]	Gewährt die Berechtigung zum Hochladen eines Anhangs für ein Angebot oder eine Bestellung	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SubmitOrderV1 [nur Berechtigung]	Gewährt die Berechtigung zum Absenden einer Bestellung	Schreiben			
TagResource [nur Berechtigung]	Gewährt die Berechtigung zum Markieren einer - AWS Elemental-Appliances-and-Software-Ressource	Tagging	quote*		
			quote		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [nur Berechtigung]	Gewährt die Berechtigung zum Entfernen eines Tags aus einer - AWS Elemental-Appliances-and-Software-Ressource	Tagging	quote*		
			quote		
				aws:TagKeys	
UpdateQuote [nur Berechtigung]	Gewährt die Berechtigung zum Ändern eines Angebots	Schreiben	quote*		

Von AWS Elemental Appliances and Software definierte Ressourcen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
quote	`arn:${Partition}:elemental-appliances-software:${Region}:${Account}:quote/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Elemental Appliances and Software

AWS Elemental Appliances and Software definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Anforderungs-Tag	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach Ressourcen-Tag	String
aws:TagKeys	Filtert den Zugriff nach Tag-Schlüsseln	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elemental Appliances and Software Activation Service

AWS Elemental Appliances and Software Activation Service (Servicepräfix: `elemental-activations`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Elemental Appliances und Software Activation Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CompleteAccountRegistration [nur Berechtigung]	Gewährt die Berechtigung, den Prozess der Registrierung des Kundenkontos für AWS-Elemental-Appliances-and-Software-Käufe abzuschließen	Read			
CompleteFileUpload [nur Berechtigung]	Gewährt die Berechtigung, das Hochladen einer Softwaredatei für AWS-Elemental-Appliances-and-Software-Käufe abzuschließen	Read			
DownloadSoftware [nur Berechtigung]	Gewährt die Berechtigung zum Downlad der Softwaredateien für AWS Elemental-Appliances-and-Software-Käufe	Read			
GenerateLicenses [nur Berechtigung]	Gewährt die Berechtigung, Softwarelizenzen für AWS-	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Elemental-Appliances-and-Software-Käufe zu generieren				
GetActivation [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben einer Aktivierung	Read	activation*		
ListTagsForResource [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Tags für eine AWS-Elemental-Activations-Ressource	Read	activation		
StartAccountRegistration [nur Berechtigung]	Gewährt die Erlaubnis, mit der Registrierung des Kundenkontos für AWS-Elemental-Appliances-and-Software-Käufe zu beginnen	Read			
StartFileUpload [nur Berechtigung]	Gewährt die Berechtigung, das Hochladen einer Softwaredatei für AWS-Elemental-Appliances-and-Software-Käufe zu starten	Read			
TagResource [nur Berechtigung]	Gewährt die Berechtigung zum Hinzufügen eines Tags für eine AWS-Elemental-Activations-Ressource	Markieren	activation*		
			activation		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource [nur Berechtigung]	Gewährt die Berechtigung zum Entfernen eines Tags aus einer AWS-Elemental-Activations-Ressource	Markieren	activation*		
			activation		
				aws:TagKeys aws:ResourceTag/${TagKey}	

Von AWS Elemental Appliances und Software Activation Service definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
activation	`arn:${Partition}:elemental-activations:${Region}:${Account}:activation/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Elemental Appliances und Software Activation Service

AWS Elemental Appliances and Software Activation Service definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch Tags, die in der Anforderung übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf Tags, die der Ressource zugeordnet sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf Tag-Schlüsseln, die in der Anforderung übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elemental MediaConnect

AWS Elemental MediaConnect (Servicepräfix: `mediaconnect`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Elemental definierte Aktionen MediaConnect

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddBridgeOutputs	Gewährt die Erlaubnis, einer bestehenden Brücke Ausgaben hinzuzufügen	Schreiben	Bridge*		
AddBridgeSources	Gewährt die Erlaubnis, einer bestehenden Brücke Quellen hinzuzufügen	Schreiben	Bridge*		
AddFlowMediaStreams	Gewährt die Berechtigung zum Hinzufügen von Medienströmen zu einem beliebigen Ablauf	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddFlowOutputs	Gewährt die Berechtigung zum Hinzufügen von Ausgaben zu einem beliebigen Ablauf.	Write			
AddFlowSources	Gewährt die Berechtigung zum Hinzufügen von Quellen zu einem beliebigen Ablauf.	Write			
AddFlowVpcInterfaces	Gewährt die Berechtigung zum Hinzufügen von VPC-Schnittstellen zu einem beliebigen Ablauf.	Schreiben			
CreateBridge	Gewährt die Berechtigung zum Erstellen von Brücken	Schreiben	Bridge*		
CreateFlow	Gewährt die Berechtigung zum Erstellen von Abläufen.	Schreiben			
CreateGateway	Gewährt die Berechtigung zum Erstellen von Gateways	Schreiben	Gateway*		
DeleteBridge	Gewährt die Berechtigung zum Löschen von Brücken	Schreiben	Bridge*		
DeleteFlow	Gewährt die Berechtigung zum Löschen von Abläufen.	Schreiben			
DeleteGateway	Gewährt die Berechtigung zum Löschen von Gateways	Schreiben	Gateway*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeregisterGatewayInstance	Gewährt die Berechtigung zum Aufheben der Registrierung einer Gateway-Instance	Schreiben	GatewayInstance*		
DescribeBridge	Gewährt die Berechtigung zum Anzeigen der Details einer Brücke	Lesen	Bridge*		
DescribeFlow	Gewährt die Berechtigung zum Anzeigen der Details eines Ablaufs, einschließlich Ablauf-ARN, Name und Availability Zone, sowie Angaben über die Quelle, Ausgaben und Berechtigungen.	Lesen			
DescribeFlowSourceMetadata	Gewährt die Berechtigung zum Anzeigen von Informationen über den Quelltransport-Stream und die Programme des Flows	Lesen			
DescribeGateway	Gewährt die Berechtigung, die Details eines Gateways anzuzeigen, einschließlich des ARN, des Namens und der CIDR-Blöcke des Gateways, sowie Details über die Netzwerke	Lesen	Gateway*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeGatewayInstance	Gewährt die Berechtigung zum Anzeigen der Details einer Gateway-Instance	Lesen	GatewayInstance*		
DescribeOffering	Gewährt die Berechtigung zum Anzeigen der Details eines Angebots.	Read			
DescribeReservation	Gewährt die Berechtigung zum Anzeigen der Details einer Reservierung.	Lesen			
DiscoverGatewayPollEndpoint	Gewährt die Berechtigung, den Gateway-Abfrage-Endpunkt zu ermitteln	Schreiben			
GrantFlowEntitlements	Gewährt die Berechtigung zum Erteilen von Berechtigungen für einen beliebigen Ablauf.	Schreiben			
ListBridges	Gewährt die Berechtigung, eine Liste der Brücken anzuzeigen, die mit diesem Konto und einem optional angegebenen ARN verknüpft sind	Auflisten	Bridge*		
ListEntitlements	Gewährt die Berechtigung zum Anzeigen einer Liste aller Berechtigungen, die dem Konto Gewährt wurden.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListFlows	Gewährt die Berechtigung zum Anzeigen einer Liste von Abläufen, die mit diesem Konto verknüpft sind.	Auflisten			
ListGatewayInstances	Gewährt die Berechtigung zum Anzeigen einer Liste von Instances, die mit diesem Gateway verknüpft sind	Auflisten	GatewayInstance*		
ListGateways	Gewährt die Berechtigung zum Anzeigen einer Liste von Gateways, die mit diesem Konto verknüpft sind	Auflisten			
ListOfferings	Gewährt die Berechtigung zum Anzeigen einer Liste aller Angebote, die dem Konto in der aktuellen AWS-Region zur Verfügung stehen	List			
ListReservations	Gewährt die Berechtigung zum Anzeigen einer Liste aller Reservierungen, die vom Konto in der aktuellen AWS-Region gekauft wurden	List			
ListTagsForResource	Gewährt die Berechtigung zum Anzeigen einer Liste von Tags, die mit einer Ressource verknüpft sind	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PollGateway	Gewährt die Berechtigung zum Abfragen eines Gateways	Schreiben			
PurchaseOffering	Gewährt die Berechtigung zum Kauf eines Angebots.	Schreiben			
RemoveBridgeOutput	Gewährt die Berechtigung, eine Ausgabe von einer bestehenden Brücke zu entfernen	Schreiben	Bridge*		
RemoveBridgeSource	Gewährt die Berechtigung, eine Quelle von einer bestehenden Brücke zu entfernen	Schreiben	Bridge*		
RemoveFlowMediaStream	Gewährt die Berechtigung zum Entfernen von Medien-Streams aus einem beliebigen Ablauf.	Write			
RemoveFlowOutput	Gewährt die Berechtigung zum Entfernen von Ausgaben aus einem beliebigen Ablauf.	Write			
RemoveFlowSource	Gewährt die Berechtigung zum Entfernen von Quellen aus einem beliebigen Ablauf.	Write			
RemoveFlowVpcInterface	Gewährt die Berechtigung zum Entfernen von VPC-Schnittstellen aus einem beliebigen Ablauf.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RevokeFlowEntitlement	Gewährt die Berechtigung zum Widerrufen von Berechtigungen für einen beliebigen Ablauf.	Write			
StartFlow	Gewährt die Berechtigung zum Starten von Abläufen.	Write			
StopFlow	Gewährt die Berechtigung zum Beenden von Abläufen.	Schreiben			
SubmitGatewayStateChange	Gewährt die Berechtigung, eine Änderung des Gateway-Status zu übermitteln	Schreiben			
TagResource	Gewährt die Berechtigung zum Verknüpfen von Tags mit Ressourcen.	Markieren			
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus Ressourcen.	Tagging			
UpdateBridge	Gewährt die Berechtigung zum Aktualisieren von Brücken	Schreiben	Bridge*		
UpdateBridgeOutput	Gewährt die Berechtigung eine Ausgabe einer bestehenden Brücke zu aktualisieren	Schreiben	Bridge*		
UpdateBridgeSource	Gewährt die Berechtigung eine Quelle einer bestehenden Brücke zu aktualisieren	Schreiben	Bridge*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateBridgeState	Gewährt die Berechtigung den Status einer bestehenden Brücke zu aktualisieren	Schreiben	Bridge*		
UpdateFlow	Gewährt die Berechtigung zum Aktualisieren von Abläufen.	Write			
UpdateFlowEntitlement	Gewährt die Berechtigung zum Aktualisieren von Berechtigungen für einen beliebigen Ablauf.	Write			
UpdateFlowMediaStream	Gewährt die Berechtigung zum Aktualisieren von Medien-Streams auf einem beliebigen Ablauf.	Write			
UpdateFlowOutput	Gewährt die Berechtigung zum Aktualisieren von Ausgaben für einen beliebigen Ablauf.	Write			
UpdateFlowSource	Gewährt die Berechtigung zum Aktualisieren der Quelle eines Ablaufs.	Schreiben			
UpdateGatewayInstance	Gewährt die Berechtigung zum Aktualisieren der Konfiguration einer bestehenden Gateway-Instance	Schreiben	GatewayInstance*		

Von AWS Elemental definierte Ressourcentypen MediaConnect

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Entitlement	`arn:${Partition}:mediaconnect:${Region}:${Account}:entitlement:${FlowId}:${EntitlementName}`	
Flow	`arn:${Partition}:mediaconnect:${Region}:${Account}:flow:${FlowId}:${FlowName}`	
Output	`arn:${Partition}:mediaconnect:${Region}:${Account}:output:${OutputId}:${OutputName}`	
Source	`arn:${Partition}:mediaconnect:${Region}:${Account}:source:${SourceId}:${SourceName}`	
Gateway	`arn:${Partition}:mediaconnect:${Region}:${Account}:gateway:${GatewayId}:${GatewayName}`	
Bridge	`arn:${Partition}:mediaconnect:${Region}:${Account}:bridge:${FlowId}:${FlowName}`	
GatewayInstance	`arn:${Partition}:mediaconnect:${Region}:${Account}:gateway:${GatewayId}:`	

Ressource ntypen	ARN	Bedingungsschlüssel
	`${GatewayName}:instance:${InstanceId}`	

Bedingungsschlüssel für AWS Elemental MediaConnect

MediaConnect besitzt keine servicespezifischen Kontextschlüssel, die im `Condition` Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elemental MediaConvert

AWS Elemental MediaConvert (Servicepräfix: `mediaconvert`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Elemental MediaConvert definierte Aktionen
- Von AWS Elemental MediaConvert definierte Ressourcentypen
- Bedingungsschlüssel für AWS Elemental MediaConvert

Von AWS Elemental MediaConvert definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen.

Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Associate Certificate	Gewährt die Berechtigung zum Zuordnen eines Amazon-Ressourcennamens (ARN) von AWS Certificate Manager (ACM) zu AWS Elemental MediaConvert	Schreiben			
CancelJob	Gewährt die Berechtigung zum Abbrechen eines AWS-Elemental-MediaConvert-Auftrags, der sich in der Warteschlange befindet.	Write	Job*		
CreateJob	Gewährt die Berechtigung zum Erstellen und Senden eines AWS-Elemental-MediaConvert-Auftrags.	Write	JobTemplate		
			Preset		
			Queue		
				aws:RequestTag/${TagKey} aws:TagKeys mediaconvert:HttpInputsAllowed mediaconvert:Https	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				InputsAllowed mediaconvert:S3InputsAllowed	
CreateJobTemplate	Gewährt die Berechtigung zum Erstellen einer benutzerdefinierten Auftragsvorlage von AWS Elemental MediaConvert.	Write	Preset Queue		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePreset	Gewährt die Berechtigung zum Erstellen einer benutzerdefinierten Ausgabevoreinstellung von AWS Elemental MediaConvert.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateQueue	Gewährt die Berechtigung zum Erstellen einer AWS-Elemental-MediaConvert-Auftragswarteschlange.	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteJobTemplate	Gewährt die Berechtigung zum Löschen einer benutzerdefinierten Auftragsvorlage von AWS Elemental MediaConvert.	Schreiben	JobTemplate*		
DeletePolicy	Gewährt die Berechtigung zum Löschen einer AWS Elemental-MediaConvert-Richtlinie	Schreiben			
DeletePreset	Gewährt die Berechtigung zum Löschen einer benutzerdefinierten Ausgabevoreinstellung von AWS Elemental MediaConvert.	Write	Preset*		
DeleteQueue	Gewährt die Berechtigung zum Löschen einer Auftragswarteschlange von AWS Elemental MediaConvert.	Write	Queue*		
DescribeEndpoints	Gewährt die Berechtigung zum Abonnieren des AWS-Elemental-MediaConvert-Service, indem eine Anforderung für einen kontospezifischen Endpunkt gesendet wird. Alle Transcodierungsanforderungen müssen an den Endpunkt gesendet werden, den der Service zurückgibt	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateCertificate	Gewährt die Berechtigung zum Entfernen einer Mapping zwischen dem Amazon-Ressourcennamen (ARN) eines AWS Certificate Manager (ACM)-Zertifikats und einer AWS Elemental-MediaConvert-Ressource	Schreiben			
GetJob	Gewährt die Berechtigung zum Abrufen eines AWS-Elemental-MediaConvert-Auftrags.	Read	Job*		
GetJobTemplate	Gewährt die Berechtigung zum Abrufen einer AWS-Elemental-MediaConvert-Auftragsvorlage.	Lesen	JobTemplate*		
GetPolicy	Gewährt die Berechtigung zum Abrufen einer AWS Elemental-MediaConvert-Richtlinie	Lesen			
GetPreset	Gewährt die Berechtigung zum Abrufen einer AWS-Elemental-MediaConvert-Ausgabevoreinstellung.	Read	Preset*		
GetQueue	Gewährt die Berechtigung zum Abrufen einer AWS-Elemental-MediaConvert-Auftragswarteschlange.	Read	Queue*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListJobTemplates	Gewährt die Berechtigung zum Auflisten von AWS-Elemental-MediaConvert-Auftragsvorlagen.	List			
ListJobs	Gewährt die Berechtigung zum Auflisten von AWS-Elemental-MediaConvert-Aufträgen.	List	Queue		
ListPresets	Gewährt die Berechtigung zum Auflisten von AWS-Elemental-MediaConvert-Ausgabevoreinstellungen.	List			
ListQueues	Gewährt die Berechtigung zum Auflisten von AWS-Elemental-MediaConvert-Auftragswarteschlangen.	List			
ListTagsForResource	Gewährt die Berechtigung zum Abrufen der Tags für eine MediaConvert-Warteschlange, einer -Voreinstellung oder einer -Auftragsvorlage.	Lesen	JobTemplate		
			Preset		
			Queue		
PutPolicy	Gewährt die Berechtigung zum Eingeben einer AWS Elemental-MediaConvert-Richtlinie	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer MediaConvert-Warteschlange, einer -Voreinstellung oder einer -Auftragsvorlage.	Markieren	JobTemplate		
			Preset		
			Queue		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer MediaConvert-Warteschlange, einer -Voreinstellung oder einer -Auftragsvorlage.	Markieren	JobTemplate		
			Preset		
			Queue		
				aws:TagKeys	
UpdateJobTemplate	Gewährt die Berechtigung zum Aktualisieren einer benutzerdefinierten AWS-Elemental-MediaConvert-Auftragsvorlage.	Write	JobTemplate*		
			Preset		
			Queue		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdatePreset	Gewährt die Berechtigung zum Aktualisieren einer benutzerdefinierten AWS-Elemental-MediaConvert-Ausgabevoreinstellung.	Write	Preset*		
UpdateQueue	Gewährt die Berechtigung zum Aktualisieren einer AWS-Elemental-MediaConvert-Auftragswarteschlange.	Write	Queue*		

Von AWS Elemental MediaConvert definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Job	`arn:${Partition}:mediaconvert:${Region}:${Account}:jobs/${JobId}`	aws:ResourceTag/${TagKey}
Queue	`arn:${Partition}:mediaconvert:${Region}:${Account}:queues/${QueueName}`	aws:ResourceTag/${TagKey}
Preset	`arn:${Partition}:mediaconvert:${Region}:${Account}:presets/${PresetName}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
JobTemplate	`arn:${Partition}:mediaconvert:${Region}:${Account}:jobTemplates/${JobTemplateName}`	aws:ResourceTag/${TagKey}
CertificateAssociation	`arn:${Partition}:mediaconvert:${Region}:${Account}:certificates/${CertificateArn}`	

Bedingungsschlüssel für AWS Elemental MediaConvert

AWS Elemental MediaConvert definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert Aktionen nach den Tag-Schlüsseln in der Anforderung	ArrayOfString

Bedingungsschlüssel	Beschreibung	Typ
mediaconvert:HttpInputsAllowed	Filtert den Zugriff anhand einer im Konto vorhandenen HTTP-Eingaberichtlinie	Bool
mediaconvert:HttpsInputsAllowed	Filtert den Zugriff anhand einer im Konto vorhandenen HTTPS-Eingaberichtlinie	Bool
mediaconvert:S3InputsAllowed	Filtert den Zugriff anhand einer im Konto vorhandenen S3-Eingaberichtlinie	Bool

Aktionen, Ressourcen und Zustandstasten für AWS Elemental MediaLive

AWS Elemental MediaLive (Dienstpräfix:`medialive`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Elemental definierte Aktionen AWS MediaLive
- Von AWS Elemental definierte Ressourcentypen MediaLive
- Zustandsschlüssel für Elemental AWS MediaLive

Von Elemental definierte Aktionen AWS MediaLive

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptInputDeviceTransfer	Gewährt die Berechtigung, die Übertragung eines Eingabegeräts zu akzeptieren	Write	input-device*		
BatchDelete	Gewährt die Berechtigung zum Löschen von Kanälen, Eingaben, Eingabesicherheitsgruppen und Multiplexen	Write			
BatchStart	Gewährt die Berechtigung zum Starten von Kanälen und Multiplexen	Write			
BatchStop	Gewährt die Berechtigung zum Beenden von Kanälen und Multiplexen	Write			
BatchUpdateSchedule	Gewährt die Berechtigung, zum Hinzufügen und Entfernen von Aktionen im Zeitplan eines Kanals	Write	channel*		
CancelInputDeviceTransfer	Gewährt die Berechtigung, die Übertragung eines Eingabegeräts abzubrechen	Schreiben	input-device*		
ClaimDevice	Gewährt die Berechtigung zum Beanspruchen eines Eingabegeräts	Schreiben	input-device*		
CreateChannel	Gewährt die Berechtigung zum Erstellen eines Channels.	Schreiben	channel* input*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudWatchAlarmTemplate	Erteilt die Erlaubnis, eine Cloudwatch-Alarmvorlage zu erstellen	Schreiben	cloudwatch-alarm-template*		
			cloudwatch-alarm-template-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudWatchAlarmTemplateGroup	Erteilt die Berechtigung zum Erstellen einer Cloudwatch-Alarm-Vorlagengruppe	Schreiben	cloudwatch-alarm-template-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateEventBridgeRuleTemplate	Erteilt die Berechtigung zum Erstellen einer Eventbridge-Regelvorlage	Schreiben	eventbridge-rule-template*		
			eventbridge-rule-template-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventBridgeRuleTemplateGroup	Erteilt die Berechtigung zum Erstellen einer Eventbridge-Regelvorlagengruppe	Schreiben	eventbridge-rule-template-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInput	Gewährt die Berechtigung zum Erstellen einer Eingabe.	Write	input*		
			input-security-group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInputSecurityGroup	Gewährt die Berechtigung zum Erstellen einer Eingabesicherheitsgruppe	Write	input-security-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMultiplex	Gewährt die Berechtigung zum Erstellen eines Multiplexes	Write	multiplex*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMultiplexProgram	Gewährt die Berechtigung zum Erstellen eines Multiplex-Programms	Schreiben	multiplex*		
CreatePartnerInput	Gewährt die Berechtigung zum Erstellen einer bestimmten Ressource	Schreiben	input*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSignalMap	Erteilt die Berechtigung zum Erstellen einer Signalmap	Schreiben	signal-map*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTags	Erteilt die Berechtigung zum Erstellen von Tags für Kanäle, Eingänge, Eingangssicherheitsgruppen, Multiplexe, Reservierungen, Signalzuordnungen, Vorlagengruppen und Vorlagen	Tagging	channel		
			cloudwatch-alarm-template		
			cloudwatch-alarm-template-group		
			eventbridge-rule-template		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			eventbridge-rule-template-group		
			input		
			input-security-group		
			multiplex		
			reservation		
			signal-map		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteChannel	Gewährt die Berechtigung zum Löschen eines Channels.	Schreiben	channel*		
DeleteCloudWatchAlarmTemplate	Erteilt die Berechtigung zum Löschen einer CloudWatch-Alarmvorlage	Schreiben	cloudwatch-alarm-template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteCloudWatchAlarmTemplateGroup	Erteilt die Berechtigung zum Löschen einer Cloudwatch-Alarm-Vorlagengruppe	Schreiben	cloudwatch-alarm-template-group*		
DeleteEventBridgeRuleTemplate	Erteilt die Berechtigung zum Löschen einer Eventbridge-Regelvorlage	Schreiben	eventbridge-rule-template*		
DeleteEventBridgeRuleTemplateGroup	Erteilt die Berechtigung zum Löschen einer Eventbridge-Regelvorlagengruppe	Schreiben	eventbridge-rule-template-group*		
DeleteInput	Gewährt die Berechtigung zum Löschen einer Eingabe.	Write	input*		
DeleteInputSecurityGroup	Gewährt die Berechtigung zum Löschen einer Eingabesicherheitsgruppe.	Write	input-security-group*		
DeleteMultiplex	Gewährt die Berechtigung zum Löschen eines Multiplexes	Write	multiplex*		
DeleteMultiplexProgram	Gewährt die Berechtigung zum Löschen eines Multiplex-Programms	Write	multiplex*		
DeleteReservation	Gewährt die Berechtigung zum Löschen einer abgelaufenen Reservierung.	Write	reservation*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteSchedule	Gewährt die Berechtigung zum Löschen aller geplanten Aktionen für einen Kanal	Schreiben	channel*		
DeleteSignalMap	Erteilt die Berechtigung zum Löschen einer Signalmap	Schreiben	signal-map*		
DeleteTags	Erteilt die Berechtigung zum Löschen von Tags aus Kanälen, Eingängen, Eingangssicherheitsgruppen, Multiplexen, Reservierungen, Signalzuordnungen, Vorlagengruppen und Vorlagen	Tagging	channel		
			cloudwatch-alarm-template		
			cloudwatch-alarm-template-group		
			eventbridge-rule-template		
			eventbridge-rule-template-group		
			input		
			input-security-group		
			multiplex		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			reservation		
			signal-map		
				aws:TagKeys	
DescribeAccountConfiguration	Erteilt die Berechtigung zum Anzeigen der Kontokonfiguration des Kunden	Lesen			
DescribeChannel	Gewährt die Berechtigung zum Abrufen von Details über einen Channel.	Read	channel*		
DescribeInput	Gewährt die Berechtigung zum Beschreiben einer Eingabe.	Read	input*		
DescribeInputDevice	Gewährt die Berechtigung zum Beschreiben eines Eingabegeräts.	Read	input-device*		
DescribeInputDeviceThumbnail	Gewährt die Berechtigung zur Beschreibung der Miniaturansicht eines Eingabegeräts	Read	input-device*		
DescribeInputSecurityGroup	Gewährt die Berechtigung zum Beschreiben einer Eingabesicherheitsgruppe.	Read	input-security-group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeMultiplex	Gewährt die Berechtigung, zum Beschreiben eines Multiplexes	Read	multiplex*		
DescribeMultiplexProgram	Gewährt die Berechtigung zum Beschreiben eines Multiplex-Programms	Read	multiplex*		
DescribeOffering	Gewährt die Berechtigung zum Abrufen von Details über ein Reservierungsangebot.	Read	offering*		
DescribeReservation	Gewährt die Berechtigung zum Abrufen von Details über eine Reservierung.	Read	reservation*		
DescribeSchedule	Gewährt die Berechtigung, eine Liste der für einen Kanal geplanten Aktionen anzuzeigen	Lesen	channel*		
DescribeThumbnails	Erteilt die Berechtigung, die Miniaturansichten für einen Channel anzusehen	Lesen	channel*		
GetCloudWatchAlarmTemplate	Erteilt die Erlaubnis, eine Cloudwatch-Alarmvorlage abzurufen	Lesen	cloudwatch-alarm-template*		
GetCloudWatchAlarmTemplateGroup	Erteilt die Berechtigung zum Abrufen einer Cloudwatch-Alarm-Vorlagengruppe	Lesen	cloudwatch-alarm-template-group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetEventBridgeRuleTemplate	Erteilt die Berechtigung zum Abrufen einer Eventbridge-Regelvorlage	Lesen	eventbridge-rule-template*		
GetEventBridgeRuleTemplateGroup	Erteilt die Berechtigung zum Abrufen einer Eventbridge-Regelvorlagengruppe	Lesen	eventbridge-rule-template-group*		
GetSignalMap	Erteilt die Berechtigung zum Abrufen einer Signalmap	Lesen	signal-map*		
ListChannels	Gewährt die Berechtigung zum Auflisten von Channels.	Auflisten			
ListCloudWatchAlarmTemplateGroups	Erteilt die Berechtigung, Cloudwatch-Alarm-Vorlagengruppen aufzulisten	Auflisten			
ListCloudWatchAlarmTemplates	Erteilt die Erlaubnis, Cloudwatch-Alarmvorlagen aufzulisten	Auflisten			
ListEventBridgeRuleTemplateGroups	Erteilt die Berechtigung, Eventbridge-Regelvorlagengruppen aufzulisten	Auflisten			
ListEventBridgeRuleTemplates	Erteilt die Berechtigung, Eventbridge-Regelvorlagen aufzulisten	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListInputDeviceTransfers	Gewährt die Berechtigung zum Auflisten der Übertragungen von Eingabegeräten	List			
ListInputDevices	Gewährt die Berechtigung zum Auflisten von Geräten.	List			
ListInputSecurityGroups	Gewährt die Berechtigung zum Auflisten von Eingabesicherheitsgruppen.	List			
ListInputs	Gewährt die Berechtigung zum Auflisten von Eingaben.	List			
ListMultiplexPrograms	Gewährt die Berechtigung zum Auflisten von Multiplex-Programmen	List			
ListMultiplexes	Gewährt die Berechtigung zum Auflisten von Multiplexen	List			
ListOfferings	Gewährt die Berechtigung zum Auflisten von Reservierungangeboten.	List			
ListReservations	Gewährt die Berechtigung zum Auflisten von Reservierungen.	Auflisten			
ListSignalMaps	Erteilt die Erlaubnis, Signalzuordnungen aufzulisten	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Erteilt die Berechtigung, Tags für Kanäle, Eingänge, Eingangssicherheitsgruppen, Multiplexe, Reservierungen, Signalzuordnungen, Vorlagengruppen und Vorlagen aufzulisten	Auflisten	channel		
			cloudwatch-alarm-template		
			cloudwatch-alarm-template-group		
			eventbridge-rule-template		
			eventbridge-rule-template-group		
			input		
			input-security-group		
			multiplex		
			reservation		
			signal-map		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PurchaseOffering	Gewährt die Berechtigung zum Kauf eines Reservierungsangebots.	Schreiben	offering*		
			reservation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RebootInputDevice	Gewährt die Berechtigung zum Neustarten eines Eingabegeräts	Schreiben	input-device*		
RejectInputDeviceTransfer	Gewährt die Berechtigung, die Übertragung eines Eingabegeräts abzulehnen	Schreiben	input-device*		
RestartChannelPipelines	Erteilt die Berechtigung, Pipelines auf einem laufenden Kanal neu zu starten	Schreiben	channel*		
StartChannel	Gewährt die Berechtigung zum Starten eines Channels.	Schreiben	channel*		
StartDeleteMonitorDeployment	Erteilt die Berechtigung, mit dem Löschen des Monitors einer Signalmap zu beginnen	Schreiben	signal-map*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartInputDevice	Erteilt die Berechtigung, ein an einen MediaConnect Flow angeschlossenes Eingabegerät zu starten	Schreiben	input-device*		
StartInputDeviceMaintenanceWindow	Gewährt die Berechtigung zum Starten eines Wartungsfensters für ein Eingabegerät	Schreiben	input-device*		
StartMonitorDeployment	Erteilt die Berechtigung, eine Signalzuordnungs-Monitor-Bereitstellung zu starten	Schreiben	signal-map*		
StartMultiplex	Gewährt die Berechtigung zum Starten eines Multiplexes	Schreiben	multiplex*		
StartUpdateSignalMap	Erteilt die Erlaubnis, ein Signal Map-Update zu starten	Schreiben	signal-map*		
StopChannel	Gewährt die Berechtigung zum Beenden eines Channels.	Schreiben	channel*		
StopInputDevice	Erteilt die Berechtigung, ein an einen MediaConnect Flow angeschlossenes Eingabegerät zu stoppen	Schreiben	input-device*		
StopMultiplex	Gewährt die Berechtigung zum Stoppen eines Multiplexes	Write	multiplex*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TransferInputDevice	Gewährt die Berechtigung zum Übertragen eines Eingabegeräts	Schreiben	input-device*		
UpdateAccountConfiguration	Erteilt die Berechtigung zum Aktualisieren einer Kundenkontokonfiguration	Schreiben			
UpdateChannel	Gewährt die Berechtigung zum Aktualisieren eines Channels.	Write	channel*		
UpdateChannelClass	Gewährt die Berechtigung zum Aktualisieren der Klasse eines Channels.	Schreiben	channel*		
UpdateCloudWatchAlarmTemplate	Erteilt die Erlaubnis, eine CloudWatch-Alarmvorlage zu aktualisieren	Schreiben	cloudwatch-alarm-template* cloudwatch-alarm-template-group*		
UpdateCloudWatchAlarmTemplateGroup	Erteilt die Berechtigung zum Aktualisieren einer Cloudwatch-Alarm-Vorlagengruppe	Schreiben	cloudwatch-alarm-template-group*		
UpdateEventBridgeRuleTemplate	Erteilt die Berechtigung zum Aktualisieren einer Eventbridge-Regelvorlage	Schreiben	eventbridge-rule-template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			eventbridge-rule-template-group*		
UpdateEventBridgeRuleTemplateGroup	Erteilt die Berechtigung zum Aktualisieren einer Eventbridge-Regelvorlagengruppe	Schreiben	eventbridge-rule-template-group*		
UpdateInput	Gewährt die Berechtigung zum Aktualisieren einer Eingabe.	Write	input*		
UpdateInputDevice	Gewährt die Berechtigung zum Aktualisieren eines Eingabegeräts.	Write	input-device*		
UpdateInputSecurityGroup	Gewährt die Berechtigung zum Aktualisieren einer Eingabesicherheitsgruppe.	Write	input-security-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateMultiplex	Gewährt die Berechtigung, ein Multiplex zu aktualisieren	Write	multiplex*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateMultiplexProgram	Gewährt die Berechtigung zum Aktualisieren eines Multiplex-Programms	Write	multiplex*		
UpdateReservation	Gewährt die Berechtigung zum Aktualisieren einer Reservierung.	Schreiben	reservation*		

Von AWS Elemental definierte Ressourcentypen MediaLive

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
channel	`arn:${Partition}:medialive:${Region}:${Account}:channel:${ChannelId}`	aws:ResourceTag/${TagKey}
input	`arn:${Partition}:medialive:${Region}:${Account}:input:${InputId}`	aws:ResourceTag/${TagKey}
input-device	`arn:${Partition}:medialive:${Region}:${Account}:inputDevice:${DeviceId}`	
input-security-group	`arn:${Partition}:medialive:${Region}:${Account}:inputSecurityGroup:${InputSecurityGroupId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
multiplex	arn:${Partition}:medialive:${Region}:${Account}:multiplex:${MultiplexId}	aws:ResourceTag/${TagKey}
reservation	arn:${Partition}:medialive:${Region}:${Account}:reservation:${ReservationId}	aws:ResourceTag/${TagKey}
offering	arn:${Partition}:medialive:${Region}:${Account}:offering:${OfferingId}	
signal-map	arn:${Partition}:medialive:${Region}:${Account}:signal-map:${SignalMapId}	aws:ResourceTag/${TagKey}
cloudwatch-alarm-template-group	arn:${Partition}:medialive:${Region}:${Account}:cloudwatch-alarm-template-group:${CloudWatchAlarmTemplateGroupId}	aws:ResourceTag/${TagKey}
cloudwatch-alarm-template	arn:${Partition}:medialive:${Region}:${Account}:cloudwatch-alarm-template:${CloudWatchAlarmTemplateId}	aws:ResourceTag/${TagKey}
eventbridge-rule-template-group	arn:${Partition}:medialive:${Region}:${Account}:eventbridge-rule-template-group:${EventBridgeRuleTemplateGroupId}	aws:ResourceTag/${TagKey}
eventbridge-rule-template	arn:${Partition}:medialive:${Region}:${Account}:eventbridge-rule-template:${EventBridgeRuleTemplateId}	aws:ResourceTag/${TagKey}

Zustandsschlüssel für Elemental AWS MediaLive

AWS Elemental MediaLive definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die

Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elemental MediaPackage

AWS Elemental MediaPackage (Servicepräfix: `mediapackage`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Elemental MediaPackage definierte Aktionen
- Von AWS Elemental MediaPackage definierte Ressourcentypen

- Bedingungsschlüssel für AWS Elemental MediaPackage

Von AWS Elemental MediaPackage definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ConfigureLogs	Gewährt die Berechtigung zum Konfigurieren von Zugriffsprotokollen für einen Kanal	Schreiben	channels*		iam:CreateServiceLinkedRole
CreateChannel	Gewährt die Berechtigung zum Erstellen eines Kanals in AWS Elemental MediaPackage.	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateHarvestJob	Gewährt die Berechtigung zum Erstellen einer Entnahmeaufgabe in AWS Elemental MediaPackage	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOriginEndpoint	Gewährt die Berechtigung zum Erstellen eines Endpunkts in AWS Elemental MediaPackage.	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Gewährt die Berechtigung zum Löschen eines Kanals in AWS Elemental MediaPackage.	Schreiben	channels*		
DeleteOriginEndpoint	Gewährt die Berechtigung zum Löschen eines Endpunkts	Schreiben	origin_endpoints*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	in AWS Elemental MediaPackage.				
DescribeChannel	Gewährt die Berechtigung zum Anzeigen der Details eines Channels in AWS Elemental MediaPackage.	Lesen	channels*		
DescribeHarvestJob	Gewährt die Berechtigung zum Anzeigen der Details einer Entnahmeaufgabe in AWS Elemental MediaPackage	Lesen	harvest_jobs*		
DescribeOriginEndpoint	Gewährt die Berechtigung zum Anzeigen der Details eines Endpunkts in AWS Elemental MediaPackage.	Lesen	origin_endpoints*		
ListChannels	Gewährt die Berechtigung zum Anzeigen einer Liste der Channels in AWS Elemental MediaPackage.	Lesen			
ListHarvestJobs	Gewährt die Berechtigung zum Anzeigen einer Liste der Entnahmeaufgaben in AWS Elemental MediaPackage	Lesen			
ListOriginEndpoints	Gewährt die Berechtigung zum Anzeigen einer Liste der Endpunkte in AWS Elemental MediaPackage.	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags, die einem Channel oder OriginEndpoint zugeordnet sind.	Lesen	channels		
			harvest_jobs		
			origin_endpoints		
RotateChannelCredentials	Gewährt die Berechtigung zum Rotieren von Anmeldeinformationen für den ersten IngestEndpoint eines Kanals in AWS Elemental MediaPackage.	Schreiben	channels*		
RotateIngestEndpointCredentials	Gewährt die Berechtigung zum Drehen von IngestEndpoint-Anmeldedaten für einen Kanal in AWS Elemental MediaPackage.	Schreiben	channels*		
TagResource	Gewährt die Berechtigung zum Markieren einer MediaPackage Ressource	Markierung	channels		
			harvest_jobs		
			origin_endpoints		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Löschen von Tags in einem Channel oder OriginEndpoint.	Markierung	channels		
			harvest_jobs		
			origin_endpoints		
				aws:TagKeys	
UpdateChannel	Gewährt die Berechtigung zum Ändern eines Channels in AWS Elemental MediaPackage.	Schreiben	channels*		
UpdateOriginEndpoint	Gewährt die Berechtigung zum Vornehmen von Änderungen an einem Endpunkt in AWS Elemental MediaPackage.	Schreiben	origin_endpoints*		

Von AWS Elemental MediaPackage definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der

Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
channels	`arn:${Partition}:mediapackage:${Region}:${Account}:channels/${ChannelIdentifier}`	aws:ResourceTag/${TagKey}
origin_endpoints	`arn:${Partition}:mediapackage:${Region}:${Account}:origin_endpoints/${OriginEndpointIdentifier}`	aws:ResourceTag/${TagKey}
harvest_jobs	`arn:${Partition}:mediapackage:${Region}:${Account}:harvest_jobs/${HarvestJobIdentifier}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Elemental MediaPackage

AWS Elemental MediaPackage definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Tag für eine MediaPackage Anforderung	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Tag für eine MediaPackage Ressource	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach den Tag-Schlüsseln für eine MediaPackage Ressource oder Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elemental MediaPackage V2

AWS Elemental MediaPackage V2 (Servicepräfix: `mediapackagev2`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Elemental MediaPackage V2 definierte Aktionen
- Von AWS Elemental MediaPackage V2 definierte Ressourcentypen
- Bedingungsschlüssel für AWS Elemental MediaPackage V2

Von AWS Elemental MediaPackage V2 definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateChannel		Schreiben	Channel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Gewährt die Berechtigung zum Erstellen eines Channels in einer Channel-Gruppe			aws:RequestTag/${TagKey} aws:TagKeys	
CreateChannelGroup	Gewährt die Berechtigung zum Erstellen einer Channel-Gruppe	Schreiben	ChannelGroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateOriginEndpoint	Gewährt die Berechtigung zum Erstellen eines Ursprungsendpunkts für einen Channel	Schreiben	OriginEndpoint*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Gewährt die Berechtigung zum Löschen eines Channels in einer Channel-Gruppe	Schreiben	Channel*		
DeleteChannelGroup	Gewährt die Berechtigung zum Löschen einer Channel-Gruppe	Schreiben	ChannelGroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteChannelPolicy	Gewährt die Berechtigung zum Löschen von Ressourcenrichtlinien von einem Channel	Schreiben	Channel*		
DeleteOriginEndpoint	Gewährt die Berechtigung zum Löschen eines Ursprungsendpunkts für einen Channel	Schreiben	OriginEndpoint*		
DeleteOriginEndpointPolicy	Gewährt die Berechtigung zum Löschen einer Ressourcenrichtlinie von einem Ursprungsendpunkt	Schreiben	OriginEndpoint*		
GetChannel	Gewährt die Berechtigung zum Abrufen der Details eines Channels in einer Channel-Gruppe	Lesen	Channel*		
GetChannelGroup	Gewährt die Berechtigung zum Abrufen der Details einer Channel-Gruppe	Lesen	ChannelGroup*		
GetChannelPolicy	Gewährt die Berechtigung zum Abrufen einer Ressourcenrichtlinie für einen Channel	Lesen	Channel*		
GetHeadObject	Gewährt die Berechtigung, GetHeadObject-Anfragen an MediaPackage zu stellen	Lesen	OriginEndpoint*		
GetObject	Gewährt die Berechtigung, GetObject-Anfragen an MediaPackage zu stellen	Lesen	OriginEndpoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetOriginEndpoint	Gewährt die Berechtigung zum Abrufen von Details zu einem Ursprungsendpunkt	Lesen	OriginEndpoint*		
GetOriginEndpointPolicy	Gewährt die Berechtigung zum Abrufen von Details zu einer Ressourcenrichtlinie für einen Ursprungsendpunkt	Lesen	OriginEndpoint*		
ListChannelGroups	Gewährt die Berechtigung zum Auflisten aller Channel-Gruppen für ein AWS-Konto	Auflisten			
ListChannels	Gewährt die Berechtigung zum Auflisten aller Channels in einer Channel-Gruppe	Auflisten	ChannelGroup*		
ListOriginEndpoints	Gewährt die Berechtigung zum Auflisten aller Ursprungsendpunkte eines Channels	Auflisten	Channel*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für die angegebene Ressource	Lesen	Channel		
			ChannelGroup		
			OriginEndpoint		
PutChannelPolicy	Gewährt die Berechtigung zum Anhängen einer Ressourcenrichtlinie für einen Channel	Schreiben	Channel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutObject	Gewährt die Berechtigung, PutObject-Anfragen an MediaPackage zu stellen	Schreiben	Channel*		
PutOriginEndpointPolicy	Gewährt die Berechtigung zum Anhängen einer Ressourcenrichtlinie an einen Ursprungsendpunkt	Schreiben	OriginEndpoint*		
TagResource	Gewährt die Berechtigung zum Hinzufügen der angegebenen Tags zur angegebenen Ressource	Markierung	Channel		
			ChannelGroup		
			OriginEndpoint		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen der angegebenen Tags aus der angegebenen Ressource	Markierung	Channel		
			ChannelGroup		
			OriginEndpoint		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateChannel	Gewährt die Berechtigung zum Aktualisieren eines Channels in einer Channel-Gruppe	Schreiben	Channel*		
UpdateChannelGroup	Gewährt die Berechtigung zum Aktualisieren einer Channel-Gruppe	Schreiben	ChannelGroup*		
UpdateOriginEndpoint	Gewährt die Berechtigung zum Aktualisieren eines Ursprungsendpunkts eines Channels	Schreiben	OriginEndpoint*		

Von AWS Elemental MediaPackage V2 definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
ChannelGroup	`arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
Channel	`arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}`	aws:ResourceTag/${TagKey}
OriginEndpoint	`arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}/originEndpoint/${OriginEndpointName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Elemental MediaPackage V2

AWS Elemental MediaPackage V2 definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch Tags, die in der Anforderung übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf Tags, die der Ressource zugeordnet sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf Tag-Schlüsseln, die in der Anforderung übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elemental MediaPackage VOD

AWS Elemental MediaPackage VOD (Servicepräfix: `mediapackage-vod`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Elemental MediaPackage VOD definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Configure Logs	Gewährt die Berechtigung zum Konfigurieren von Zugangsprotokollen für eine PackagingGroup	Schreiben	packaging-groups*		iam:CreateServiceLinkedRole
CreateAsset	Gewährt die Berechtigung zum Erstellen einer Komponente in AWS Elemental MediaPackage.	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreatePackagingConfiguration	Gewährt die Berechtigung zum Erstellen einer Verpackungskonfiguration in AWS Elemental MediaPackage.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePackagingGroup	Gewährt die Berechtigung zum Erstellen einer Verpackungsgruppe in AWS Elemental MediaPackage.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAsset	Gewährt die Berechtigung zum Löschen einer Komponente in AWS Elemental MediaPackage.	Write	assets*		
DeletePackagingConfiguration	Gewährt die Berechtigung zum Löschen einer Verpackungskonfiguration in AWS Elemental MediaPackage.	Write	packaging-configurations*		
DeletePackagingGroup	Gewährt die Berechtigung zum Löschen einer Verpackungsgruppe in AWS Elemental MediaPackage.	Write	packaging-groups*		
DescribeAsset	Gewährt die Berechtigung zum Anzeigen der Details einer Komponente in AWS Elemental MediaPackage.	Read	assets*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribePackagingConfiguration	Gewährt die Berechtigung zum Anzeigen der Details einer Verpackungskonfiguration in AWS Elemental MediaPackage.	Read	packaging-configurations*		
DescribePackagingGroup	Gewährt die Berechtigung zum Anzeigen der Details einer Verpackungsgruppe in AWS Elemental MediaPackage.	Read	packaging-groups*		
ListAssets	Gewährt die Berechtigung zum Anzeigen einer Liste der Komponenten in AWS Elemental MediaPackage.	List			
ListPackagingConfigurations	Gewährt die Berechtigung zum Anzeigen einer Liste von Verpackungskonfigurationen in AWS Elemental MediaPackage.	List			
ListPackagingGroups	Gewährt die Berechtigung zum Anzeigen einer Liste der Verpackungsgruppen in AWS Elemental MediaPackage.	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags, die einer PackagingGroup, PackagingConfiguration oder einer Komponente zugewiesen sind.	Lesen	assets		
			packaging-configurations		
			packaging-groups		
TagResource	Gewährt die Berechtigung zum Zuweisen von Tags zu einer PackagingGroup, PackagingConfiguration oder einer Komponente.	Markierung	assets		
			packaging-configurations		
			packaging-groups		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Löschen von Tags aus einer PackagingGroup, PackagingConfiguration oder Komponente.	Markierung	assets		
			packaging-configurations		
			packaging-groups		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
UpdatePackagingGroup	Gewährt die Berechtigung zum Aktualisieren einer Verpackungsgruppe in AWS Elemental MediaPackage	Write	packaging-groups*		

Von AWS Elemental MediaPackage VOD definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
assets	`arn:${Partition}:mediapackage-vod:${Region}:${Account}:assets/${AssetIdentifier}`	aws:ResourceTag/${TagKey}
packaging-configurations	`arn:${Partition}:mediapackage-vod:${Region}:${Account}:packaging-configurations/${PackagingConfigurationIdentifier}`	aws:ResourceTag/${TagKey}
packaging-groups	`arn:${Partition}:mediapackage-vod:${Region}:${Account}:packaging-groups/${PackagingGroupIdentifier}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Elemental MediaPackage VOD

AWS Elemental MediaPackage VOD definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung.	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf den Tag-Schlüssel-Wert-Paaren, die an die Ressource angefügt wurden.	Zeichenfolge
aws:TagKeys	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elemental MediaStore

AWS Elemental MediaStore (Servicepräfix: `mediastore`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Elemental MediaStore definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateContainer	Erteilt die Berechtigung zum Erstellen eines Containers	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteContainer	Gewährt die Berechtigung zum Löschen eines Containers	Schreiben	container*		
DeleteContainerPolicy	Gewährt die Berechtigung zum Löschen der Zugriffsrichtlinie eines Containers	Berechtigungsverwaltung	container*		
DeleteCorsPolicy	Gewährt die Berechtigung zum Löschen der CORS-Richtlinie eines Containers	Schreiben	container*		
DeleteLifecyclePolicy	Gewährt die Berechtigung zum Löschen der Lebenszyklusrichtlinie eines Containers	Schreiben	container*		
DeleteMetricPolicy	Gewährt die Berechtigung zum Löschen der Metrikrichtlinie eines Containers	Schreiben	container*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteObject	Gewährt die Berechtigung zum Löschen eines Objekts	Schreiben	object*		
DescribeContainer	Gewährt die Berechtigung zum Abrufen von Details zu einem Container	Auflisten	container*		
DescribeObject	Gewährt die Berechtigung zum Abrufen von Metadaten für ein Objekt	Auflisten	object*		
GetContainerPolicy	Gewährt die Berechtigung zum Abrufen der Zugriffsrichtlinie eines Containers	Lesen	container*		
GetCorsPolicy	Gewährt die Berechtigung zum Abrufen der CORS-Richtlinie eines Containers	Lesen	container*		
GetLifecyclePolicy	Gewährt die Berechtigung zum Abrufen der Lebenszyklusrichtlinie, die einem Container zugewiesen wurde	Lesen	container*		
GetMetricPolicy	Gewährt die Berechtigung zum Abrufen der Metrikrichtlinie, die einem Container zugewiesen wurde	Lesen	container*		
GetObject	Gewährt die Berechtigung zum Abrufen eines Objekts	Lesen	object*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListContainers	Gewährt die Berechtigung zum Abrufen einer Liste mit Containern im aktuellen Konto	Auflisten			
ListItems	Gewährt die Berechtigung zum Abrufen einer Liste mit Objekten und Unterordnern, die in einem Ordner gespeichert sind	Auflisten	folder		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags in einem Container	Lesen	container		
PutContainerPolicy	Gewährt die Berechtigung zum Erstellen oder Ersetzen der Zugriffsrichtlinie eines Containers	Berechtigungsverwaltung	container*		
PutCorsPolicy	Gewährt die Berechtigung zum Hinzufügen oder Ändern der CORS-Richtlinie eines Containers	Schreiben	container*		
PutLifecyclePolicy	Gewährt die Berechtigung zum Hinzufügen oder Ändern der Lebenszyklusrichtlinie, die einem Container zugewiesen wurde	Schreiben	container*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutMetricPolicy	Gewährt die Berechtigung zum Hinzufügen oder Ändern der Metrikrichtlinie, die einem Container zugewiesen wurde	Schreiben	container*		
PutObject	Gewährt die Berechtigung zum Hochladen eines Objekts	Schreiben	object*		
StartAccessLogging	Gewährt die Berechtigung zum Starten der Zugriffsprotokollierung eines Containers	Schreiben	container*		iam:PassRole
StopAccessLogging	Gewährt die Berechtigung zum Stoppen der Zugriffsprotokollierung eines Containers	Schreiben	container*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einem Container	Markierung	container		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags von einem Container	Markierung	container		
				aws:TagKeys	

Von AWS Elemental MediaStore definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
container	`arn:${Partition}:mediastore:${Region}:${Account}:container/${ContainerName}`	aws:ResourceTag/${TagKey}
object	`arn:${Partition}:mediastore:${Region}:${Account}:container/${ContainerName}/${ObjectPath}`	
folder	`arn:${Partition}:mediastore:${Region}:${Account}:container/${ContainerName}/${FolderPath}`	

Bedingungsschlüssel für AWS Elemental MediaStore

AWS Elemental MediaStore definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elemental MediaTailor

AWS Elemental MediaTailor (Servicepräfix: `mediatailor`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Elemental MediaTailor definierte Aktionen
- Von AWS Elemental MediaTailor definierte Ressourcentypen
- Bedingungsschlüssel für AWS Elemental MediaTailor

Von AWS Elemental MediaTailor definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ConfigureLogsForChannel	Gewährt die Berechtigung, Protokolle für den Kanal mit dem angegebenen Kanalnamen zu konfigurieren	Schreiben	channel*		
ConfigureLogsForPlaybackConfiguration	Gewährt die Berechtigung zum Konfigurieren von Protokollen für eine Wiedergabekonfiguration	Schreiben	playbackConfiguration*		iam:CreateServiceLinkedRole
CreateChannel	Gewährt die Berechtigung zum Erstellen eines Channels.	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLiveSource	Gewährt die Berechtigung zum Erstellen einer neuen Live-Quelle am Quellspeicherort mit dem angegebenen Quellspeicherortnamen	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePrefetchSchedule	Gewährt die Berechtigung zum Erstellen eines Prefetch-Zeitplans für die Wiedergabekonfiguration mit dem angegebenen Wiedergabekonfigurationsnamen	Schreiben	playbackConfiguration*		
CreateProgram	Gewährt die Berechtigung zum Erstellen eines neuen	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Programms auf dem Kanal mit dem angegebenen Kanalnamen				
CreateSourceLocation	Gewährt die Berechtigung zum Erstellen eines neuen Quellspeicherorts	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateVodSource	Gewährt die Berechtigung zum Erstellen einer neuen VOD-Quelle am Quellspeicherort mit dem angegebenen Quellspeicherort	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Gewährt Berechtigungen zum Löschen des Ziels mit dem angegebenen Namen	Schreiben	channel*		
DeleteChannelPolicy	Gewährt die Berechtigung zum Löschen der IAM-Richtlinie auf dem Kanal mit dem angegebenen Kanalnamen	Berechtigungsverwaltung	channel*		
DeleteLiveSource	Gewährt die Berechtigung zum Löschen der Live-Quelle mit dem angegebenen Live-Quellnamen am Quellspeicherort mit dem angegebenen Quellspeicherortnamen	Schreiben	liveSource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeletePlaybackConfiguration	Gewährt die Berechtigung zum Löschen der angegebenen Wiedergabekonfiguration	Schreiben	playbackConfiguration*		
DeletePrefetchSchedule	Gewährt die Berechtigung zum Löschen eines Prefetch-Zeitplans für eine Wiedergabekonfiguration mit dem angegebenen Prefetch-Zeitplannamen	Schreiben	playbackConfiguration*		
			prefetchSchedule*		
DeleteProgram	Gewährt die Berechtigung, das Programm mit dem angegebenen Programmnamen auf dem Kanal mit dem angegebenen Kanalnamen zu löschen	Schreiben	program*		
DeleteSourceLocation	Gewährt die Berechtigung zum Löschen des Quellorts mit dem angegebenen Quellspeicherort	Schreiben	sourceLocation*		
DeleteVodSource	Gewährt die Berechtigung zum Löschen der VOD-Quelle mit dem angegebenen VOD-Quellnamen am Quellspeicherort mit dem angegebenen Quellspeicherort	Schreiben	vodSource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeChannel	Gewährt die Berechtigung zum Abrufen des Kanals mit dem angegebenen Kanalnamen	Lesen	channel*		
DescribeLiveSource	Gewährt die Berechtigung zum Abrufenen der Live-Quelle mit dem angegebenen Live-Quellnamen am Quellspeicherort mit dem angegebenen Quellspeicherortnamen	Lesen	liveSource*		
DescribeProgram	Gewährt die Berechtigung zum Abrufen des Programms mit dem angegebenen Programmnamen auf dem Kanal mit dem angegebenen Kanalnamen	Lesen	program*		
DescribeSourceLocation	Gewährt die Berechtigung zum Abrufen des Quellorts mit dem angegebenen Quellspeicherort	Lesen	sourceLocation*		
DescribeVodSource	Gewährt die Berechtigung zum Abrufen der VOD-Quelle mit dem angegebenen VOD-Quellnamen am Quellspeicherort mit dem angegebenen Quellspeicherort	Lesen	vodSource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetChannelPolicy	Gewährt die Berechtigung zum Lesen der IAM-Richtlinie auf dem Kanal mit dem angegebenen Kanalnamen	Lesen	channel*		
GetChannelSchedule	Gewährt die Berechtigung zum Abrufen des Zeitplans von Programmen auf dem Kanal mit dem angegebenen Kanalnamen	Lesen	channel*		
GetPlaybackConfiguration	Gewährt die Berechtigung zum Abrufen der Konfiguration für den angegebenen Namen.	Lesen	playbackConfiguration*		
GetPrefetchSchedule	Gewährt die Berechtigung zum Abrufen eines Prefetch-Zeitplans für eine Wiedergabekonfiguration mit dem angegebenen Prefetch-Zeitplannamen	Lesen	playbackConfiguration* prefetchSchedule*		
ListAlerts	Gewährt die Berechtigung zum Abrufen einer Liste der Ressourcendefinitionen.	Lesen			
ListChannels	Gewährt die Berechtigung zum Abrufen eines bestehenden Bot-Channels	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListLiveSources	Gewährt die Berechtigung zum Abrufen der Liste der vorhandenen Love-Quellen am Quellspeicherort mit dem angegebenen Quellspeicherortnamen	Lesen			
ListPlaybackConfigurations	Gewährt die Berechtigung zum Abrufen der Liste der verfügbaren Konfigurationen.	Auflisten			
ListPrefetchSchedules	Gewährt die Berechtigung zum Abrufen der Liste von Prefetch-Zeitplänen für eine Wiedergabekonfiguration	Auflisten	playbackConfiguration*		
ListSourceLocations	Gewährt die Berechtigung zum Abrufen der Liste der vorhandenen Quellorte	Lesen			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags, die der angegebenen Wiedergabekonfigurationsressource zugeordnet sind	Lesen	channel		
			liveSource		
			playbackConfiguration		
			sourceLocation		
			vodSource		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListVodSources	Gewährt die Berechtigung zum Abrufen der Liste der vorhandenen VOD-Quellen am Quellspeicherort mit dem angegebenen Quellspeicherort	Lesen			
PutChannelPolicy	Gewährt die Berechtigung zum Festlegen der IAM-Richtlinie für den Kanal mit dem angegebenen Kanalnamen	Berechtigungsverwaltung	channel*		
PutPlaybackConfiguration	Gewährt die Berechtigung zum Hinzufügen einer neuen Konfiguration.	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
StartChannel	Gewährt die Berechtigung, den Kanal mit dem angegebenen Kanalnamen zu starten	Schreiben	channel*		
StopChannel	Gewährt die Berechtigung, den Kanal mit dem angegebenen Kanalnamen zu stoppen	Schreiben	channel*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zur angegebenen Wiedergabekonfigurationsressource	Markierung	channel		
			liveSource		
			playbackConfiguration		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			sourceLocation		
			vodSource		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus der angegebenen Wiedergabekonfigurationsressource	Markierung	channel		
			liveSource		
			playbackConfiguration		
			sourceLocation		
			vodSource		
				aws:TagKeys	
UpdateChannel	Gewährt die Berechtigung zum Aktualisieren des Kanals mit dem angegebenen Kanalnamen.	Schreiben	channel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateLiveSource	Gewährt die Berechtigung zum Aktualisieren der Live-Quelle mit dem angegebenen Live-Quellnamen am Quellspeicherort mit dem angegebenen Quellspeicherortnamen	Schreiben	liveSource*		
UpdateProgram	Gewährt die Berechtigung, das Programm mit dem angegebenen Programmnamen auf dem Kanal mit dem angegebenen Kanalnamen zu aktualisieren	Schreiben	program*		
UpdateSourceLocation	Gewährt die Berechtigung zum Aktualisieren des Quellorts mit dem angegebenen Quellspeicherort	Schreiben	sourceLocation*		
UpdateVodSource	Gewährt die Berechtigung zum Aktualisieren der VOD-Quelle mit dem angegebenen VOD-Quellnamen am Quellspeicherort mit dem angegebenen Quellspeicherort	Schreiben	vodSource*		

Von AWS Elemental MediaTailor definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
playbackConfiguration	`arn:${Partition}:mediatailor:${Region}:${Account}:playbackConfiguration/${ResourceId}`	aws:ResourceTag/${TagKey}
prefetchSchedule	`arn:${Partition}:mediatailor:${Region}:${Account}:prefetchSchedule/${ResourceId}`	
channel	`arn:${Partition}:mediatailor:${Region}:${Account}:channel/${ChannelName}`	aws:ResourceTag/${TagKey}
program	`arn:${Partition}:mediatailor:${Region}:${Account}:program/${ChannelName}/${ProgramName}`	
sourceLocation	`arn:${Partition}:mediatailor:${Region}:${Account}:sourceLocation/${SourceLocationName}`	aws:ResourceTag/${TagKey}
vodSource	`arn:${Partition}:mediatailor:${Region}:${Account}:vodSource/${SourceLocationName}/${VodSourceName}`	aws:ResourceTag/${TagKey}
liveSource	`arn:${Partition}:mediatailor:${Region}:${Account}:liveSource/${SourceLocationName}/${LiveSourceName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Elemental MediaTailor

AWS Elemental MediaTailor definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden,

um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für elementare Supportfälle für AWS

Elementare Supportfälle für AWS (Service-Präfix: `elemental-support-cases`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von elementare Supportfälle für AWS definierte Aktionen
- Von elementaren Supportfällen für AWS definierte Ressourcentypen

- Bedingungsschlüssel für elementare Supportfälle für AWS

Von elementare Supportfälle für AWS definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CheckCasePermission [nur Berechtigung]	Gewährt die Berechtigung zu überprüfen, ob der Anrufer über die Berechtigung zum Ausführen von Supportfallvorgängen verfügt	Schreiben			
CreateCase [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines Suppotfalls	Schreiben			
GetCase [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben eines Supportfalls in Ihrem Konto	Lesen			
GetCases [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der Supportfälle in Ihrem Konto	Lesen			
UpdateCase [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren eines Supportfalls	Schreiben			

Von elementaren Supportfällen für AWS definierte Ressourcentypen

Elementare Supportfälle für AWS unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf elementare Supportfälle für AWS zu ermöglichen, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für elementare Supportfälle für AWS

Elemental Support Cases hat keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen

Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Elemental Support Content

AWS Elemental Support Content (Service-Präfix: `elemental-support-content`) stellen die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungsschlüssel zur Verfügung, die in IAM-Richtlinien zur Berechtigung verwendet werden können.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Elemental Support Content definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich

sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Query [nur Berechtigung]	Gewährt die Berechtigung zum Durchsuchen von Supportinhalten	Lesen			

Von AWS Elemental Support Content definierte Ressourcentypen

AWS Elemental Support Content unterstützen nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf AWS Elemental Support Content zu ermöglichen, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Elemental Support Content

Elemental Support Content hat keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EMR in EKS (EMR-Container)

Amazon EMR in EKS (EMR-Container) (Servicepräfix: `emr-containers`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon EMR in EKS (EMR-Container) definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt,

müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelJobRun	Gewährt die Berechtigung, die Ausführung einer Aufgabe abzubrechen	Schreiben	jobRun*		
CreateJobTemplate	Gewährt die Berechtigung zum Erstellen einer Auftragsvorlage.	Schreiben		aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
CreateManagedEndpoint	Gewährt die Berechtigung zum Erstellen eines verwalteten Endpunkts	Schreiben	virtualCluster*		
				aws:RequestTag/${TagKey} aws:TagKeys emr-containers:ExecutionRoleArn	
CreateSecurityConfiguration	Gewährt die Berechtigung zum Erstellen einer Sicherheitskonfiguration.	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateVirtualCluster	Gewährt die Berechtigung zum Erstellen eines virtuellen Clusters	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteJobTemplate	Gewährt die Berechtigung zum Löschen einer Auftragsvorlage.	Schreiben	jobTemplate*		
DeleteManagedEndpoint	Gewährt die Berechtigung zum Löschen eines verwalteten Endpunkts	Write	managedEndpoint*		
DeleteVirtualCluster	Gewährt die Berechtigung zum Löschen eines virtuellen Clusters	Write	virtualCluster*		
DescribeJobRun	Gewährt die Berechtigung zum Beschreiben der Ausführung einer Aufgabe	Lesen	jobRun*		
DescribeJobTemplate	Gewährt die Berechtigung zum Beschreiben einer Auftragsvorlage.	Lesen	jobTemplate*		
DescribeManagedEndpoint	Gewährt die Berechtigung zum Beschreiben eines verwalteten Endpunkts	Lesen	managedEndpoint*		
DescribeSecurityConfiguration	Erteilt die Erlaubnis, eine Sicherheitskonfiguration zu beschreiben	Lesen	securityConfiguration*		
DescribeVirtualCluster	Gewährt die Berechtigung zur Beschreibung eines virtuellen Clusters	Lesen	virtualCluster*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetManagedEndpointSessionCredentials	Gewährt die Berechtigung, ein Sitzungs-Token zu erzeugen, das zur Verbindung mit einem verwalteten Endpunkt verwendet wird	Schreiben	managedEndpoint*		
ListJobRuns	Gewährt die Berechtigung zum Auflisten von Aufgabenausführungen, die einem virtuellen Cluster zugeordnet sind	Auflisten	virtualCluster*		
ListJobTemplates	Gewährt die Berechtigung zum Auflisten von Auftragsvorlagen.	Auflisten			
ListManagedEndpoints	Gewährt die Berechtigung zum Auflisten von verwalteten Endpunkten, die einem virtuellen Cluster zugeordnet sind	Auflisten	virtualCluster*		
ListSecurityConfigurations	Gewährt die Berechtigung zum Auflisten von Sicherheitskonfigurationen	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für die angegebene Ressource	List	jobRun		
			jobTemplate		
			managedEndpoint		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			virtualCluster		
ListVirtualClusters	Gewährt die Berechtigung zum Auflisten virtueller Cluster	List			
StartJobRun	Gewährt die Berechtigung zum Starten einer Aufgabenausführung	Write	virtualCluster*		
				aws:RequestTag/${TagKey} aws:TagKeys emr-containers:ExecutionRoleArn emr-containers:JobTemplateArn	
TagResource	Gewährt die Berechtigung zum Markieren der angegebenen Ressource	Markieren	jobRun		
			jobTemplate		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			managedEndpoint		
			virtualCluster		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung der angegebenen Ressource	Markieren	jobRun		
			jobTemplate		
			managedEndpoint		
			virtualCluster		
				aws:TagKeys	

Von Amazon EMR in EKS (EMR-Container) definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
virtualCluster	`arn:${Partition}:emr-containers:${Region}:${Account}:/virtualclusters/${VirtualClusterId}`	aws:ResourceTag/${TagKey}
jobRun	`arn:${Partition}:emr-containers:${Region}:${Account}:/virtualclusters/${VirtualClusterId}/jobruns/${JobRunId}`	aws:ResourceTag/${TagKey}
jobTemplate	`arn:${Partition}:emr-containers:${Region}:${Account}:/jobtemplates/${JobTemplateId}`	aws:ResourceTag/${TagKey}
managedEndpoint	`arn:${Partition}:emr-containers:${Region}:${Account}:/virtualclusters/${VirtualClusterId}/endpoints/${EndpointId}`	aws:ResourceTag/${TagKey}
securityConfiguration	`arn:${Partition}:emr-containers:${Region}:${Account}:/securityconfigurations/${SecurityConfigurationId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon EMR in EKS (EMR-Container)

Amazon EMR in EKS (EMR-Container) definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tag-Schlüssel-Wert-Paare, die in der Anforderung vorhanden sind	String
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüsselwertpaaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung	ArrayOfString
emr-containers:ExecutionRoleArn	Filtert den Zugriff nach der in der Anforderung vorhanden en Ausführungsrolle	ARN
emr-containers:JobTemplateArn	Filtert den Zugriff nach der Auftragsvorlage die in der Anforderung vorhandenen ist	ARN

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EMR Serverless

Amazon EMR Serverless (Servicepräfix: `emr-serverless`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon EMR Serverless definierte Aktionen
- Von Amazon EMR Serverless definierte Ressourcentypen
- Bedingungsschlüssel für Amazon EMR Serverless

Von Amazon EMR Serverless definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AccessInteractiveEndpoints [nur Berechtigung]	Gewährt die Berechtigung zum Ausführen interaktiver Workloads in einer Anwendung	Schreiben	application*		iam:PassRole
CancelJobRun	Gewährt die Berechtigung, die Ausführung einer Aufgabe abzubrechen	Schreiben	jobRun*		
CreateApplication	Erteilt die Berechtigung zum Erstellen einer Anwendung	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Gewährt die Berechtigung zum Löschen einer Anwendung	Schreiben	application*		
GetApplication	Erteilt die Berechtigung zum Abrufen einer Anwendung	Lesen	application*		
GetDashboardForJobRun	Erteilt die Berechtigung zum Abrufen eines Auftragsausführungs-Dashboards	Lesen	jobRun*		
GetJobRun	Erteilt die Berechtigung zum Abrufen einer Auftragsausführung	Lesen	jobRun*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListApplications	Gewährt die Berechtigung zum Auflisten von Anwendungen	Auflisten			
ListJobRuns	Erteilt die Berechtigung zum Auflisten von Auftragsausführungen, die einer Anwendung zugeordnet sind	Auflisten	application*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für die angegebene Ressource	Lesen	application		
			jobRun		
StartApplication	Erteilt die Berechtigung zum Starten einer Anwendung	Schreiben	application*		
StartJobRun	Gewährt die Berechtigung zum Starten einer Aufgabenausführung	Schreiben	application*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
StopApplication	Erteilt die Berechtigung zum Beenden einer Anwendung	Schreiben	application*		
TagResource	Gewährt die Berechtigung zum Markieren der angegebenen Ressource	Markieren	application		
			jobRun		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung der angegebenen Ressource	Markierung	application		
			jobRun		
				aws:TagKeys	
UpdateApplication	Erteilt die Berechtigung zum Aktualisieren einer Anwendung	Schreiben	application*		

Von Amazon EMR Serverless definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
application	`arn:${Partition}:emr-serverless:${Region}:${Account}:/applications/${ApplicationId}`	aws:ResourceTag/${TagKey}
jobRun	`arn:${Partition}:emr-serverless:${Region}:${Account}:/applications/${ApplicationId}/jobruns/${JobRunId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon EMR Serverless

Amazon EMR Serverless definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Entity Resolution

AWS Entity Resolution (Dienstpräfix:`entityresolution`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Entity Resolution definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddPolicyStatement	Erteilt die Erlaubnis, einem AWS Dienst oder einem anderen Konto die Erlaubnis zur Nutzung von AWS Entity Resolution-Ressourcen zu erteilen	Berechtigungsverwaltung			
CreateIdMappingWorkflow	Gewährt die Berechtigung zum Erstellen eines idmapping-Workflows	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateIdNamespace	Erteilt die Erlaubnis zum Erstellen eines IdNamespace	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMatchingWorkflow	Gewährt die Berechtigung zum Erstellen eines Übereinstimmungs-Workflows	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSchemaMapping	Gewährt die Berechtigung zum Erstellen einer Schemazuordnung	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteIdMappingWorkflow	Gewährt die Berechtigung zum Löschen eines idmapping-Workflows	Schreiben	IdMappingWorkflow*		
DeleteIdNamespace	Erteilt die Erlaubnis zum Löschen eines IdNamespace	Schreiben	IdNamespace*		
DeleteMatchingWorkflow	Gewährt die Berechtigung zum Löschen eines Übereinstimmungs-Workflows	Schreiben	MatchingWorkflow*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeletePolicyStatement	Löscht die einem AWS Dienst oder einem anderen Konto erteilte Berechtigung zur Nutzung von AWS Entity Resolution-Ressourcen	Berechtigungsverwaltung			
DeleteSchemaMapping	Gewährt die Berechtigung zum Löschen einer Schemazuordnung	Schreiben	SchemaMapping*		
GetIdMappingJob	Gewährt die Berechtigung zum Abrufen eines idmapping-Auftrags	Lesen	IdMappingWorkflow*		
GetIdMappingWorkflow	Gewährt die Berechtigung zum Abrufen eines idmapping-Workflows	Lesen	IdMappingWorkflow*		
GetIdNamespace	Erteilt die Erlaubnis, eine zu erhalten IdNamespace	Lesen	IdNamespace*		
GetMatchId	Gewährt die Berechtigung zum Abrufen einer Übereinstimmungs-ID	Lesen	MatchingWorkflow*		
GetMatchingJob	Gewährt die Berechtigung zum Abrufen einer Übereinstimmungsaufgabe	Lesen	MatchingWorkflow*		
GetMatchingWorkflow	Gewährt die Berechtigung zum Abrufen eines Übereinstimmungs-Workflows	Lesen	MatchingWorkflow*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetPolicy	Ruft eine Ressourcenrichtlinie für eine AWS Entität ab. Ressourcen	Lesen			
GetProviderService	Gewährt die Berechtigung zum Abrufen des Providerservices	Lesen	ProviderService*		
GetSchemaMapping	Gewährt die Berechtigung zum Abrufen einer Schemazuordnung	Lesen	SchemaMaping*		
ListIdMappingJobs	Gewährt die Berechtigung zum Auflisten von idmapping-Aufträgen	Auflisten	IdMappingWorkflow*		
ListIdMappingWorkflows	Gewährt die Berechtigung zum Auflisten von idmapping-Workflows	Auflisten			
ListIdNamespaces	Erteilt die Erlaubnis zum Auflisten IdNamespaces	Auflisten			
ListMatchingJobs	Gewährt die Berechtigung zum Auflisten von Übereinstimmungsaufträgen	Auflisten	MatchingWorkflow*		
ListMatchingWorkflows	Gewährt die Berechtigung zum Auflisten von Übereinstimmungs-Workflows	Auflisten			
ListProviderServices	Gewährt die Berechtigung zum Auflisten von Providerservices	Auflisten	ProviderService*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListSchemaMappings	Gewährt die Berechtigung zum Auflisten von Schemazuordnungen	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen			
PutPolicy	Legen Sie eine Ressourcenrichtlinie für Ressourcen für AWS Entity Resolution fest	Berechtigungsverwaltung			
StartIdMappingJob	Gewährt die Berechtigung zum Starten eines idmapping-Auftrags	Schreiben	IdMappingWorkflow*		
StartMatchingJob	Gewährt die Berechtigung zum Starten einer Übereinstimmungsaufgabe	Schreiben	MatchingWorkflow*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Ressource	Tagging		aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Tagging		aws:TagKeys	
UpdateIdMappingWorkflow	Gewährt die Berechtigung zum Aktualisieren eines idmapping-Workflows	Schreiben	IdMappingWorkflow*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateIdNamespace	Erteilt die Erlaubnis zur Aktualisierung eines IdNamespace	Schreiben	IdNamespace*		
UpdateMatchingWorkflow	Gewährt die Berechtigung zum Aktualisieren eines Übereinstimmungs-Workflows	Schreiben	MatchingWorkflow*		
UpdateSchemaMapping	Gewährt die Berechtigung zum Aktualisieren einer Schemazuordnung	Schreiben	SchemaMapping*		
UseIdNamespace	Erteilt die Berechtigung, einem AWS Dienst oder einem anderen Konto die Erlaubnis zur Verwendung IdNamespace innerhalb eines Workflows zu erteilen	Berechtigungsverwaltung			

Von AWS Entity Resolution definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
MatchingWorkflow	`arn:${Partition}:entityresolution::${Account}:matchingworkflow/${WorkflowName}`	aws:ResourceTag/${TagKey}
SchemaMapping	`arn:${Partition}:entityresolution::${Account}:schemamapping/${SchemaName}`	aws:ResourceTag/${TagKey}
IdMappingWorkflow	`arn:${Partition}:entityresolution::${Account}:idmappingworkflow/${WorkflowName}`	aws:ResourceTag/${TagKey}
ProviderService	`arn:${Partition}:entityresolution::${Account}:providerservice/${ProviderName}/${ProviderServiceName}`	aws:ResourceTag/${TagKey}
IdNamespace	`arn:${Partition}:entityresolution::${Account}:idnamespace/${IdNamespaceName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Entity Resolution

AWS Entity Resolution definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff entsprechend eines Schlüssels, der in der Anforderung vorhanden ist, die der Benutzer an den Entity-Resolution-Service sendet	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff anhand eines Tag-Schlüssel-Wert-Paares	String
aws:TagKeys	Filtert den Zugriff nach der Liste aller Tag-Schlüsselnamen, die in der Anforderung vorhanden sind, die der Benutzer an den Entity-Resolution-Service sendet	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EventBridge

Amazon EventBridge (Service-Präfix:`events`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon definierte Aktionen EventBridge
- Von Amazon definierte Ressourcentypen EventBridge
- Zustandsschlüssel für Amazon EventBridge

Von Amazon definierte Aktionen EventBridge

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen.

Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ActivateEventSource	Gewährt die Berechtigung zum Aktivieren von Partner-Ereignisquellen	Write	event-source*		
CancelReplay	Gewährt die Berechtigung zum Abbrechen einer erneuten Wiedergabe	Write	replay*		
CreateApiDestination	Gewährt die Berechtigung zum Erstellen eines neuen API-Ziels	Write	api-destination*		
			connection*		
CreateArchive	Gewährt die Berechtigung zum Erstellen eines neuen Archivs	Write	archive*		
			event-bus*		
CreateConnection	Gewährt die Berechtigung zum Erstellen einer neuen Verbindung	Schreiben	connection*		
CreateEndpoint	Gewährt die Berechtigung zum Erstellen eines Endpunkts	Schreiben	endpoint*		
				events:EventBusArn	
CreateEventBus	Gewährt die Berechtigung zum Erstellen von Ereignisbussen	Write	event-bus*		
				aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
CreatePartnerEventSource	Gewährt die Berechtigung zum Erstellen von Partner-Ereignisquellen	Write	event-source*		
DeactivateEventSource	Gewährt die Berechtigung zum Deaktivieren von Ereignisquellen	Write	event-source*		
DeauthorizeConnection	Gewährt die Berechtigung die Autorisierung einer Verbindung aufzuheben, wobei ihre gespeicherten Autorisierungs-Secrets gelöscht werden	Write	connection*		
DeleteApiDestination	Gewährt die Berechtigung zum Löschen eines API-Ziels	Write	api-destination*		
DeleteArchive	Gewährt die Berechtigung zum Löschen eines Archivs	Write	archive*		
DeleteConnection	Gewährt die Berechtigung zum Löschen einer Verbindung.	Schreiben	connection*		
DeleteEndpoint	Gewährt die Berechtigung zum Löschen eines Endpunkts	Schreiben	endpoint*		
DeleteEventBus	Gewährt die Berechtigung zum Löschen von Ereignisbussen	Write	event-bus*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeletePartnerEventSource	Gewährt die Berechtigung zum Löschen von Partner-Ereignisquellen	Write	event-source*		
DeleteRule	Gewährt die Berechtigung zum Löschen von Regeln	Write	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount events:ManagedBy	
DescribeApiDestination	Gewährt die Berechtigung zum Abrufen von Details zu einem API-Ziel	Read	api-destination*		
			connection*		
DescribeArchive	Gewährt die Berechtigung zum Abrufen von Details zu einem Archiv	Read	archive*		
DescribeConnection	Gewährt die Berechtigung zum Abrufen von Details zu einer Verbindung	Lesen	connection*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeEndpoint	Gewährt die Berechtigung zum Abrufen von Details zu einem Endpunkt	Lesen	endpoint*		
DescribeEventBus	Gewährt die Berechtigung zum Abrufen von Details zu Ereignisbussen	Read	event-bus		
DescribeEventSource	Gewährt die Berechtigung zum Abrufen von Details zu Ereignisquellen	Read	event-source*		
DescribePartnerEventSource	Gewährt die Berechtigung zum Abrufen von Details zu Partner-Ereignisquellen	Read	event-source*		
DescribeReplay	Gewährt die Berechtigung zum Abrufen der Details einer erneuten Wiedergabe	Read	replay*		
DescribeRule	Gewährt die Berechtigung zum Abrufen von Details zu Regeln	Read	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisableRule	Gewährt die Berechtigung zum Deaktivieren von Regeln	Schreiben	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount events:ManagedBy	
EnableRule	Gewährt die Berechtigung zum Aktivieren von Regeln	Schreiben	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount events:ManagedBy	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
InvokeApiDestination [nur Berechtigung]	Gewährt die Berechtigung zum Aufrufen eines API-Ziels	Write	api-destination*		
ListApiDestinations	Gewährt die Berechtigung zum Abrufen einer Liste von API-Zielen	List			
ListArchives	Gewährt die Berechtigung zum Abrufen einer Liste von Archiven	List			
ListConnections	Gewährt die Berechtigung zum Abrufen einer Liste von Verbindungen.	Auflisten			
ListEndpoints	Gewährt die Berechtigung zum Abrufen einer Liste von Endpunkten	Auflisten			
ListEventBuses	Gewährt die Berechtigung zum Abrufen einer Liste der Ereignisbusse in Ihrem Konto	Auflisten			
ListEventSources	Gewährt die Berechtigung zum Abrufen einer Liste von Ereignisquellen, die mit diesem Konto geteilt werden	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListPartnerEventSourceAccounts	Erteilt die Erlaubnis, eine Liste von AWS-Konto IDs abzurufen, die einer Ereignisquelle zugeordnet sind	Auflisten	event-source*		
ListPartnerEventSources	Gewährt die Berechtigung zum Abrufen einer Liste von Partner-Ereignisquellen	List			
ListReplays	Gewährt die Berechtigung zum Abrufen einer Liste erneuter Wiedergaben	List			
ListRuleNamesByTarget	Gewährt die Berechtigung zum Abrufen einer Liste der Namen von Regeln, die einem Ziel zugeordnet sind	Auflisten			
ListRules	Erteilt die Erlaubnis, eine Liste der EventBridge Amazon-Regeln im Konto abzurufen	Auflisten			
ListTagsForResource	Erteilt die Erlaubnis, eine Liste von Tags abzurufen, die mit einer EventBridge Amazon-Ressource verknüpft sind	Auflisten	event-bus		
			rule-on-custom-event-bus		
			rule-on-default-event-bus		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				events:creatorAccount	
ListTargetsByRule	Gewährt die Berechtigung zum Abrufen einer Liste von Zielen, die für eine Regel definiert sind	Auflisten	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount	
PutEvents	Erteilt die Erlaubnis, benutzerdefinierte Ereignisse an Amazon zu senden EventBridge	Schreiben	event-bus*		
				events:detail-type events:source events:eventBusInvocation	
PutPartnerEvents	Erteilt die Erlaubnis, benutzerdefinierte Ereignisse an Amazon zu senden EventBridge	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutPermission	Erteilt die Erlaubnis, die PutPermission Aktion zu verwenden, um einer anderen Person die Erlaubnis AWS-Konto zu erteilen, Ereignisse in Ihren Standard-Event-Bus zu übertragen	Berechtigungsverwaltung			
PutRule	Gewährt die Berechtigung zum Erstellen oder Aktualisieren von Regeln	Schreiben	rule-on-custom-event-bus		
			rule-on-default-event-bus		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				events:detail.userIdentity.principalId events:detail-type events:source events:detail.service events:detail.eventTypeCode aws:RequestTag/${TagKey} aws:TagKeys events:creatorAccount events:ManagedBy	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutTargets	Gewährt die Berechtigung zum Hinzufügen von Zielen zu einer Regel	Schreiben	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:TargetArn events:creatorAccount events:ManagedBy	
RemovePermission	Erteilt die Erlaubnis, einer anderen Person die Erlaubnis AWS-Konto zu entziehen, Ereignisse in Ihren Standard-Event-Bus zu übertragen	Berechtigungsverwaltung			
RemoveTargets	Gewährt die Berechtigung, Ziele aus einer Regel zu entfernen	Schreiben	rule-on-custom-event-bus		
			rule-on-default-event-bus		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				events:creatorAccount events:ManagedBy	
RetrieveConnectionCredentials [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Anmeldeinformationen zu einer Verbindung	Schreiben	connection*		
StartReplay	Gewährt die Berechtigung, die erneute Wiedergabe eines Archivs zu starten	Schreiben	archive*		
			event-bus*		
			replay*		
TagResource	Erteilt die Erlaubnis, einer EventBridge Amazon-Ressource ein Tag hinzuzufügen	Tagging	event-bus		
			rule-on-custom-event-bus		
			rule-on-default-event-bus		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey} events:creatorAccount	
TestEventPattern	Gewährt die Berechtigung zum Testen, ob ein Ereignismuster mit dem bereitgestellten Ereignis übereinstimmt	Lesen			
UntagResource	Erteilt die Erlaubnis, ein Tag aus einer EventBridge Amazon-Ressource zu entfernen	Tagging	event-bus		
			rule-on-custom-event-bus		
			rule-on-default-event-bus		
				aws:TagKeys events:creatorAccount	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateApiDestination	Gewährt die Berechtigung zum Aktualisieren eines API-Ziels	Write	api-destination*		
UpdateArchive	Gewährt die Berechtigung zum Aktualisieren eines Archivs	Write	archive*		
UpdateConnection	Gewährt die Berechtigung zum Aktualisieren einer Verbindung.	Schreiben	connection*		
UpdateEndpoint	Gewährt die Berechtigung zum Aktualisieren eines Endpunkts	Schreiben	endpoint*		
				events:EventBusArn	
UpdateEventBus	Erteilt die Erlaubnis, Event-Busse zu aktualisieren	Schreiben	event-bus*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Von Amazon definierte Ressourcentypen EventBridge

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
event-source	`arn:${Partition}:events:${Region}::event-source/${EventSourceName}`	
event-bus	`arn:${Partition}:events:${Region}:${Account}:event-bus/${EventBusName}`	aws:ResourceTag/${TagKey}
rule-on-default-event-bus	`arn:${Partition}:events:${Region}:${Account}:rule/${RuleName}`	aws:ResourceTag/${TagKey}
rule-on-custom-event-bus	`arn:${Partition}:events:${Region}:${Account}:rule/${EventBusName}/${RuleName}`	aws:ResourceTag/${TagKey}
archive	`arn:${Partition}:events:${Region}:${Account}:archive/${ArchiveName}`	
replay	`arn:${Partition}:events:${Region}:${Account}:replay/${ReplayName}`	
connection	`arn:${Partition}:events:${Region}:${Account}:connection/${ConnectionName}`	
api-destination	`arn:${Partition}:events:${Region}:${Account}:api-destination/${ApiDestinationName}`	
endpoint	`arn:${Partition}:events:${Region}:${Account}:endpoint/${EndpointName}`	

Zustandsschlüssel für Amazon EventBridge

Amazon EventBridge definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff auf Event Bus- und Regelaktionen basierend auf dem Satz an zulässigen Werten für jedes Tag	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff auf Event Bus- und Regelaktionen basierend auf dem Tag-Wert, der der Ressource zugeordnet ist	String
aws:TagKeys	Filtert den Zugriff auf Event Bus- und Regelaktionen basierend auf den Tags in der Anforderung	ArrayOfString
events:EventBusArn	Filtert den Zugriff nach dem ARN der Event-Busse, die einem Endpunkt zugeordnet werden können, CreateEndpoint und UpdateEndpoint Aktionen	ArrayOfARN
events:ManagedBy	Filtert den Zugriff nach AWS Diensten. Wenn eine Regel von einem AWS Dienst in Ihrem Namen erstellt wird, entspricht der Wert dem Prinzipalnamen des Dienstes, der die Regel erstellt hat	String
events:TargetArn	Filtert den Zugriff nach dem ARN eines Ziels, das einer Regel für PutTargets Aktionen zugewiesen werden kann. TargetARN beinhaltet nicht DeadLetterConfigArn	ArrayOfARN
events:creatorAccount	Filtert den Zugriff auf Regelaktionen basierend auf dem Konto, in dem die Regel erstellt wurde	String

Bedingungsschlüssel	Beschreibung	Typ
events:detail-type	Filtert den Zugriff anhand der Literalzeichenfolge des Detailtyps des Ereignisses und der Aktionen PutEvents PutRule	String
events:detail.eventTypeCode	Filtert den Zugriff nach der Literalzeichenfolge für das Detail. eventTypeCode Feld des Ereignisses bis hin zu Aktionen PutRule	String
events:detail.service	Filtert den Zugriff auf Aktionen anhand der Literalzeichenfolge für das Feld detail.service des Ereignisses PutRule	String
events:detail.userIdentity.principalId	Filtert den Zugriff auf Aktionen anhand der Literalzeichenfolge für das Feld detail.useridentity.principalid des Ereignisses PutRule	String
events:eventBusInvocation	Filtert den Zugriff danach, ob das Ereignis über eine API oder einen kontenübergreifenden Busaufruf von Aktionen generiert wurde PutEvents	String
events:source	Filtert den Zugriff nach der AWS Service- oder AWS Partnerereignisquelle, die das Ereignis generiert hat, PutEvents und PutRule nach Aktionen. Entspricht der Literalzeichenfolge des Quellfelds des Ereignisses	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EventBridge Pipes

Amazon EventBridge Pipes (Servicepräfix: `pipes`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.

- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon EventBridge Pipes definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreatePipe	Gewährt die Berechtigung zum Erstellen einer Pipe	Schreiben	pipe*		iam:PassRole
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeletePipe	Gewährt die Berechtigung zum Löschen einer Pipe	Schreiben	pipe*		
				aws:ResourceTag/${TagKey}	
DescribePipe	Gewährt die Berechtigung zum Beschreiben einer Pipe	Lesen	pipe*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
ListPipes	Gewährt die Berechtigung zum Auflisten aller Pipes in Ihrem Konto	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für eine Ressource	Lesen	pipe*		
				aws:ResourceTag/${TagKey}	
StartPipe	Gewährt die Berechtigung zum Starten einer Pipe	Schreiben	pipe*		
				aws:ResourceTag/${TagKey}	
StopPipe	Gewährt die Berechtigung zum Stoppen einer Pipe	Schreiben	pipe*		
				aws:ResourceTag/${TagKey}	
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Ressource	Markieren	pipe*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Ressource	Markierung	pipe*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdatePipe	Gewährt die Berechtigung zum Aktualisieren einer Pipe	Schreiben	pipe*		iam:PassRole
				aws:ResourceTag/${TagKey}	

Von der Amazon EventBridge Pipes definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
pipe	`arn:${Partition}:pipes:${Region}:${Account}:pipe/${Name}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon EventBridge Pipes

Amazon EventBridge Pipes definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den zulässigen Werten für jedes der Tags	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Tag-Wert, der der Ressource zugeordnet ist	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach dem Vorhandensein verbindlicher Tags in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EventBridge Scheduler

Amazon EventBridge Scheduler (Servicepräfix: `scheduler`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon EventBridge Scheduler definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSchedule	Gewährt die Berechtigung zum Erstellen eines Plans von Amazon EventBridge Scheduler	Schreiben	schedule*		iam:PassRole
				aws:ResourceTag/${TagKey}	
CreateScheduleGroup	Gewährt die Berechtigung zum Erstellen eines Plans von einer Gruppe von Amazon EventBridge Scheduler	Schreiben	schedule-group*		
				aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
DeleteSchedule	Gewährt die Berechtigung zum Löschen eines Plans von Amazon EventBridge Scheduler	Schreiben	schedule*		
				aws:ResourceTag/${TagKey}	
DeleteScheduleGroup	Gewährt die Berechtigung zum Löschen eines Plans einer Gruppe von Amazon EventBridge Scheduler	Schreiben	schedule-group*		scheduler:DeleteSchedule
				aws:ResourceTag/${TagKey}	
GetSchedule	Gewährt die Berechtigung zum Anzeigen der Details zu einem Plan von Amazon EventBridge Scheduler	Lesen	schedule*		
				aws:ResourceTag/${TagKey}	
GetScheduleGroup	Gewährt die Berechtigung zum Anzeigen der Details zu einer Plangruppe von Amazon EventBridge Scheduler	Lesen	schedule-group*		
				aws:ResourceTag/${TagKey}	
ListScheduleGroups	Gewährt die Berechtigung zum Auflisten der Plangruppen von Amazon EventBridge Scheduler in Ihrem Konto	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListSchedules	Gewährt die Berechtigung zum Auflisten der Pläne von Amazon EventBridge Scheduler in Ihrem Konto	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource von Amazon EventBridge Scheduler	Lesen	schedule-group		
				aws:ResourceTag/${TagKey}	
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource von Amazon EventBridge Scheduler	Markierung	schedule-group*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UntagResource	Gewährt die Berechtigung zum Entfernen eine Markierung einer Ressource von Amazon EventBridge Scheduler	Markierung	schedule-group*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateSchedule	Gewährt die Berechtigung zum Ändern eines Plans von Amazon EventBridge Scheduler	Schreiben	schedule*		iam:PassRole
				aws:ResourceTag/${TagKey}	

Von Amazon EventBridge Scheduler definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
schedule-group	`arn:${Partition}:scheduler:${Region}:${Account}:schedule-group/${GroupName}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
schedule	`arn:${Partition}:scheduler:${Region}:${Account}:schedule/${GroupName}/${ScheduleName}`	

Bedingungsschlüssel für Amazon EventBridge Scheduler

Amazon EventBridge Scheduler definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert Aktionen nach den Tag-Schlüsseln in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EventBridge Schemas

Amazon EventBridge (Servicepräfix: `schemas`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon EventBridge Schemas definierte Aktionen
- Von Amazon EventBridge-Schemas definierte Ressourcentypen
- Bedingungsschlüssel für Amazon EventBridge Schemas

Von Amazon EventBridge Schemas definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDiscoverer	Gewährt die Berechtigung zum Erstellen eines Ereignisschema-Discoverers. Einmal erstellt, werden Ihre Ereignisse automatisch in die entsprechenden Schema-Dokumente eingeblendet.	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRegistry	Gewährt die Berechtigung zum Erstellen einer neuen Schema Registry in Ihrem Konto	Schreiben	registry*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSchema	Gewährt die Berechtigung zum Erstellen eines neuen Schemas in Ihrem Konto	Schreiben	schema*		
				aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
DeleteDiscoverer	Gewährt die Berechtigung zum Löschen von Discoverer in Ihrem Konto	Schreiben	discoverer*		
DeleteRegistry	Gewährt die Berechtigung zum Löschen einer vorhandenen Registry in Ihrem Konto	Schreiben	registry*		
DeleteResourcePolicy	Gewährt die Berechtigung zum Löschen der ressourcenbasierten Richtlinie, die an eine bestimmte Registry angefügt ist	Schreiben	registry*		
DeleteSchema	Gewährt die Berechtigung zum Löschen eines vorhandenen Schemas in Ihrem Konto	Schreiben	schema*		
DeleteSchemaVersion	Gewährt die Berechtigung zum Löschen einer bestimmten Version des Schemas in Ihrem Konto	Schreiben	schema*		
DescribeCodeBinding	Gewährt die Berechtigung zum Abrufen von Metadaten für generierten Code für ein bestimmtes Schema in Ihrem Konto	Lesen	schema*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDiscoverer	Gewährt die Berechtigung zum Abrufen von Discoverer-Metadaten in Ihrem Konto	Lesen	discoverer*		
DescribeRegistry	Gewährt die Berechtigung zum Beschreiben vorhandener Registry-Metadaten in Ihrem Konto	Lesen	registry*		
DescribeSchema	Gewährt die Berechtigung zum Abrufen eines vorhandenen Schemas in Ihrem Konto	Lesen	schema*		
ExportSchema	Gewährt die Berechtigung zum Exportieren der AWS Registry oder erkannter Schemas im OpenAPI-3-Format ins JSONSchema-Format	Lesen	registry* schema*		
GetCodeBindingSource	Gewährt die Berechtigung zum Abrufen von Metadaten für generierten Code für ein bestimmtes Schema in Ihrem Konto	Lesen	schema*		
GetDiscoveredSchema	Gewährt die Berechtigung zum Abrufen eines Schemas für die bereitgestellte Liste von Beispielereignissen	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetResourcePolicy	Gewährt die Berechtigung zum Abrufen der ressourcenbasierten Richtlinie, die an eine bestimmte Registry angefügt ist	Lesen	registry*		
ListDiscoverers	Gewährt die Berechtigung zum Auflisten aller Discoverer in Ihrem Konto	Auflisten	discoverer*		
ListRegistries	Gewährt die Berechtigung zum Auflisten aller Registrys in Ihrem Konto	Auflisten	registry*		
ListSchemaVersions	Gewährt die Berechtigung zum Auflisten aller Versionen eines Schemas	Auflisten	schema*		
ListSchemas	Gewährt die Berechtigung zum Auflisten aller Schemas	Auflisten	schema*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen	discoverer		
			registry		
			schema		
PutCodeBinding	Gewährt die Berechtigung zum Generieren von Code für ein bestimmtes Schema in Ihrem Konto	Schreiben	schema*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutResourcePolicy	Gewährt die Berechtigung zum Anfügen einer ressourcenbasierten Richtlinie an eine bestimmte Registry	Schreiben	registry*		
SearchSchemas	Gewährt die Berechtigung zum Durchsuchen von Schemas auf der Grundlage von angegebenen Schlüsselwörtern in Ihrem Konto	Auflisten	schema*		
StartDiscoverer	Gewährt die Berechtigung zum Starten des angegebenen Discoverers Nach dem Start registriert der Discoverer automatisch Schemata für veröffentlichte Ereignisse an der konfigurierten Quelle in Ihrem Konto.	Schreiben	discoverer*		
StopDiscoverer	Gewährt die Berechtigung zum Anhalten des angegebenen Discoverers Nach dem Anhalten registriert der Discoverer keine Schemata mehr für veröffentlichte Ereignisse an der konfigurierten Quelle in Ihrem Konto	Schreiben	discoverer*		
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markierung	discoverer		
			registry		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			schema		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen eines Tags von einer Ressource	Markierung	discoverer		
			registry		
			schema		
				aws:TagKeys	
UpdateDiscoverer	Gewährt die Berechtigung zum Aktualisieren eines vorhandenen Discoverers in Ihrem Konto	Schreiben	discoverer*		
UpdateRegistry	Gewährt die Berechtigung zum Aktualisieren vorhandener Registry-Metadaten in Ihrem Konto	Schreiben	registry*		
UpdateSchema	Gewährt die Berechtigung zum Aktualisieren eines vorhandenen Schemas in Ihrem Konto	Schreiben	schema*		

Von Amazon EventBridge-Schemas definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
discoverer	`arn:${Partition}:schemas:${Region}:${Account}:discoverer/${DiscovererId}`	aws:ResourceTag/${TagKey}
registry	`arn:${Partition}:schemas:${Region}:${Account}:registry/${RegistryName}`	aws:ResourceTag/${TagKey}
schema	`arn:${Partition}:schemas:${Region}:${Account}:schema/${RegistryName}/${SchemaName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon EventBridge Schemas

Amazon EventBridge Schemas definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den zulässigen Werten für jedes der Tags	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Tag-Wert, der der Ressource zugeordnet ist	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach dem Vorhandensein verbindlicher Tags in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Fault Injection Service

AWS Fault Injection Service (Servicepräfix: `fis`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Vom AWS Fault Injection Service definierte Aktionen
- Vom AWS Fault Injection Service definierte Ressourcentypen
- Bedingungsschlüssel für AWS Fault Injection Service

Vom AWS Fault Injection Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateExperimentTemplate	Gewährt die Berechtigung zum Erstellen einer AWS-FIS-Versuchsvorlage	Schreiben	action*		
			experiment-template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTargetAccountConfiguration	Gewährt die Berechtigung zum Erstellen einer AWS-FIS-Zielkontokonfiguration	Schreiben	experiment-template*		
DeleteExperimentTemplate	Gewährt die Berechtigung zum Löschen der AWS-FIS-Versuchsvorlage	Schreiben	experiment-template*		
DeleteTargetAccountConfiguration	Gewährt die Berechtigung zum Löschen einer AWS-FIS-Zielkontokonfiguration	Schreiben	experiment-template*		
GetAction	Gewährt die Berechtigung zum Abrufen einer AWS-FIS-Aktion	Read	action*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetExperiment	Gewährt die Erlaubnis zum Abrufen eines AWS-FIS-Experiments	Lesen	experiment*		
				aws:ResourceTag/${TagKey}	
GetExperimentTargetAccountConfiguration	Gewährt die Berechtigung zum Abrufen einer AWS-FIS-Zielkontokonfiguration für ein AWS-FIS-Experiment	Lesen	experiment*		
GetExperimentTemplate	Gewährt die Berechtigung zum Abrufen einer AWS-FIS-Versuchsvorlage	Lesen	experiment-template*		
				aws:ResourceTag/${TagKey}	
GetTargetAccountConfiguration	Gewährt die Berechtigung zum Abrufen einer AWS-FIS-Zielkontokonfiguration für eine AWS-FIS-Experimentvorlage	Lesen	experiment-template*		
GetTargetResourceType	Erteilt die Berechtigung zum Abrufen von Informationen über den angegebenen Ressourcentyp	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
InjectApiInternalError [nur Berechtigung]	Gewährt die Erlaubnis, einen internen API-Fehler für den bereitgestellten AWS-Service aus einem FIS-Experiment zu injizieren	Schreiben	experiment*		
				fis:Service fis:Operations fis:Percentage fis:Targets	
InjectApiThrottleError [nur Berechtigung]	Gewährt die Erlaubnis, einen API-Drosselfehler für den bereitgestellten AWS-Service aus einem FIS-Experiment zu injizieren	Schreiben	experiment*		
				fis:Service fis:Operations fis:Percentage fis:Targets	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
InjectApiUnavailableError [nur Berechtigung]	Gewährt die Erlaubnis, einen nicht verfügbaren API-Fehler für den bereitgestellten AWS-Service aus einem FIS-Experiment zu injizieren	Write	experiment*		
				fis:Service fis:Operations fis:Percentage fis:Targets	
ListActions	Gewährt die Berechtigung, alle verfügbaren AWS-FIS-Aktionen aufzulisten	Auflisten			
ListExperimentResolvedTargets	Gewährt die Berechtigung zum Auflisten gelöster Ziele für AWS-FIS-Experimente	Auflisten	experiment*		
ListExperimentTargetAccountConfigurations	Gewährt die Berechtigung zum Auflisten von Zielkonto konfigurationen für AWS-FIS-Experimente	Auflisten	experiment*		
ListExperimentTemplates	Gewährt die Berechtigung zum Auflisten aller verfügbaren AWS-FIS-Versuchsvorlagen	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListExperiments	Gewährt die Berechtigung, alle verfügbaren AWS-FIS-Experimente aufzulisten	Auflisten			
ListTagsForResource	Erteilt die Berechtigung zum Auflisten der Tags für eine AWS-FIS-Ressource.	Lesen	action		
			experiment		
			experiment-template		
ListTargetAccountConfigurations	Gewährt die Berechtigung zum Auflisten von Zielkonto konfigurationen für AWS-FIS-Experimentvorlagen	Auflisten	experiment-template*		
ListTargetResourceTypes	Erteilt die Berechtigung zum Auflisten der Ressourcentypen	Auflisten			
StartExperiment	Gewährt die Berechtigung zum Ausführen eines AWS-FIS-Experiments	Write	experiment*		iam:CreateServiceLinkedRole
			experiment-template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
StopExperiment	Gewährt die Erlaubnis, ein AWS-FIS-Experiment zu beenden	Write	experiment*		
TagResource	Gewährt die Berechtigung zum Markieren von AWS-FIS-Ressourcen	Markieren	action		
			experiment		
			experiment-template		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung von AWS-FIS-Ressourcen	Markieren	action		
			experiment		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			experiment-template		
				aws:TagKeys	
UpdateExperimentTemplate	Gewährt die Berechtigung zum Aktualisieren der angegebenen AWS-FIS-Versuchsvorlage	Schreiben	experiment-template*		
			action		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTargetAccountConfiguration	Gewährt die Berechtigung zum Aktualisieren einer AWS-FIS-Zielkontokonfiguration	Schreiben	experiment-template*		

Vom AWS Fault Injection Service definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
action	`arn:${Partition}:fis:${Region}:${Account}:action/${Id}`	aws:ResourceTag/${TagKey}
experiment	`arn:${Partition}:fis:${Region}:${Account}:experiment/${Id}`	aws:ResourceTag/${TagKey}
experiment-template	`arn:${Partition}:fis:${Region}:${Account}:experiment-template/${Id}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Fault Injection Service

AWS Fault Injection Service definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wertepaaren, die in der Anforderung zulässig sind	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paar einer Ressource	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach Liste von Tag-Schlüsseln, die in der Anforderung zulässig sind	ArrayOfString
fis:Operations	Filtert den Zugriff über die Liste der Vorgänge im AWS-Service, die von der AWS-FIS-Aktion betroffen sind	ArrayOfString

Bedingungsschlüssel	Beschreibung	Typ
fis:Percentage	Filtert den Zugriff nach dem Prozentsatz der Anrufe, die von der AWS-FIS-Aktion betroffen sind	Numerischer Wert
fis:Service	Filtert den Zugriff durch den AWS-Service, der von der AWS-FIS-Aktion betroffen ist	Zeichenfolge
fis:Targets	Filtert den Zugriff nach der Liste der Ressourcen-ARNs, die von der AWS-FIS-Aktion angegriffen werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon FinSpace

Amazon FinSpace (Service-Präfix:`finspace`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon definierte Aktionen FinSpace
- Von Amazon definierte Ressourcentypen FinSpace
- Zustandsschlüssel für Amazon FinSpace

Von Amazon definierte Aktionen FinSpace

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ConnectKxCluster [nur Berechtigung]	Gewährt die Berechtigung zum Herstellen einer Verbindung zu einem KDB-Cluster	Schreiben	kxCluster*		
CreateEnvironment	Erteilt die Erlaubnis, eine FinSpace Umgebung zu erstellen	Schreiben	environment*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxChangeset	Gewährt die Berechtigung zum Erstellen eines Changesets für eine KDB-Datenbank	Schreiben	kxDatabase*		
CreateKxCluster	Gewährt die Berechtigung zum Erstellen eines Clusters in einer verwalteten KDB-Umgebung	Schreiben	kxCluster*		ec2:DescribeSubnets finspace:MountKxDatabase
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey}	
CreateKxDatabase	Gewährt die Berechtigung zum Erstellen einer KDB-Datenbank in einer verwalteten KDB-Umgebung	Schreiben	kxDatabase*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxDataview	Gewährt die Berechtigung zum Erstellen einer Datenansicht in einer verwalteten kdb-Umgebung	Schreiben	kxDataview*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxEnvironment	Gewährt die Berechtigung zum Erstellen einer verwalteten KDB-Umgebung	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxScalingGroup	Gewährt die Berechtigung zum Erstellen einer Skalierungsgruppe in einer verwalteten kdb-Umgebung	Schreiben	kxScalingGroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxUser	Gewährt die Berechtigung zum Erstellen eines Benutzers in einer verwalteten KDB-Umgebung	Schreiben	kxEnvironment*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxVolume	Gewährt die Berechtigung zum Erstellen eines Volumes in einer verwalteten kdb-Umgebung	Schreiben	kxVolume*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateUser	Erteilt die Erlaubnis, einen FinSpace Benutzer zu erstellen	Schreiben	environment*		
			user*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteEnvironment	Erteilt die Erlaubnis, eine FinSpace Umgebung zu löschen	Schreiben	environment*		
DeleteKxCluster	Gewährt die Berechtigung zum Löschen eines KDB-Clusters	Schreiben	kxCluster*		
DeleteKxClusterNode	Erteilt die Erlaubnis, einen Knoten aus einem KDB-Cluster zu löschen	Schreiben	kxCluster*		
DeleteKxDatabase	Gewährt die Berechtigung zum Löschen einer KDB-Datenbank	Schreiben	kxDatabase*		
DeleteKxDataview	Gewährt die Berechtigung zum Löschen einer Datenansicht in einer verwalteten kdb-Umgebung	Schreiben	kxDataview*		
DeleteKxEnvironment	Gewährt die Berechtigung zum Löschen einer verwalteten KDB-Umgebung	Schreiben	kxEnvironment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteKxScalingGroup	Gewährt die Berechtigung zum Löschen einer Skalierungsgruppe in einer verwalteten kdb-Umgebung	Schreiben	kxScalingGroup*		
DeleteKxUser	Gewährt die Berechtigung zum Löschen eines KDB-Benutzers	Schreiben	kxUser*		
DeleteKxVolume	Gewährt die Berechtigung zum Löschen eines Volumes in einer verwalteten kdb-Umgebung	Schreiben	kxVolume*		
GetEnvironment	Erteilt die Erlaubnis, eine FinSpace Umgebung zu beschreiben	Lesen	environment*		
GetKxChangeset	Gewährt die Berechtigung zum Beschreiben eines Changesets für eine KDB-Datenbank	Lesen	kxDatabase*		
GetKxCluster	Gewährt die Berechtigung zum Beschreiben eines Clusters in einer verwalteten KDB-Umgebung	Lesen	kxCluster*		
GetKxConnectionString	Gewährt die Berechtigung zum Abrufen einer Verbindungszeichenfolge für KDB-Cluster	Lesen	kxCluster*		finspace:ConnectKxCluster

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetKxDatabase	Gewährt die Berechtigung zum Beschreiben einer KDB-Datenbank	Lesen	kxDatabase*		
GetKxDataview	Gewährt die Berechtigung zum Beschreiben einer Datenansicht in einer verwalteten KDB-Umgebung	Lesen	kxDataview*		
GetKxEnvironment	Gewährt die Berechtigung zum Beschreiben einer verwalteten KDB-Umgebung	Lesen	kxEnvironment*		
GetKxScalingGroup	Gewährt die Berechtigung zum Beschreiben einer Skalierungsgruppe in einer verwalteten kdb-Umgebung	Lesen	kxScalingGroup*		
GetKxUser	Gewährt die Berechtigung zum Beschreiben eines KDB-Nutzers	Lesen	kxUser*		
GetKxVolume	Gewährt die Berechtigung zum Beschreiben eines Volumes in einer verwalteten kdb-Umgebung	Lesen	kxVolume*		
GetLoadSampleDataSetGroupIntoEnvironmentStatus	Gewährt die Berechtigung zum Abfragen des Ladestatus eines Beispieldatenpakets	Lesen	environment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetUser	Erteilt die Erlaubnis, einen FinSpace Benutzer zu beschreiben	Lesen	environment*		
			user*		
ListEnvironments	Erteilt die Erlaubnis, FinSpace Umgebungen aufzulisten in AWS-Konto	Auflisten	environment*		
ListKxChangesets	Gewährt die Berechtigung zum Auflisten eines Changesets für eine KDB-Datenbank	Auflisten	kxDatabase*		
ListKxClusterNodes	Gewährt die Berechtigung zum Auflisten eines Cluster-Knotens in einer verwalteten KDB-Umgebung	Auflisten	kxCluster*		
ListKxClusters	Gewährt die Berechtigung zum Auflisten eines Clusters in einer verwalteten KDB-Umgebung	Auflisten	kxEnvironment*		
ListKxDatabases	Gewährt die Berechtigung zum Auflisten einer KDB-Darenbank in einer verwaltet en KDB-Umgebung	Auflisten	kxEnvironment*		
ListKxDataviews	Gewährt die Berechtigung zum Auflisten von Datenansichten in einer Datenbank	Auflisten	kxDatabase*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListKxEnvironments	Gewährt die Berechtigung zum Auflisten von verwalteten KDB-Umgebungen	Auflisten			
ListKxScalingGroups	Gewährt die Berechtigung zum Auflisten von Skalierungsgruppen in einer verwalteten kdb-Umgebung	Auflisten	kxEnvironment*		
ListKxUsers	Gewährt die Berechtigung zum Auflisten von Benutzern in einer verwalteten KDB-Umgebung	Auflisten	kxEnvironment*		
ListKxVolumes	Gewährt die Berechtigung zum Auflisten von Volumes in einer verwalteten kdb-Umgebung	Auflisten	kxEnvironment*		
ListTagsForResource	Gewährt Berechtigungen zum Zurückgeben einer Liste der Tags für eine Ressource	Auflisten	environment*		
			kxCluster*		
			kxDatabase*		
			kxDataview*		
			kxEnvironment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			kxScalingGroup*		
			kxUser*		
			kxVolume*		
ListUsers	Erteilt die Berechtigung, FinSpace Benutzer in einer Umgebung aufzulisten	Auflisten	environment*		
			user*		
LoadSampleDataSetGroupIntoEnvironment	Erteilt die Erlaubnis, ein Beispieldatenpaket in Ihre FinSpace Umgebung zu laden	Schreiben	environment*		
MountKxDatabase [nur Berechtigung]	Gewährt die Berechtigung zum Mounten einer Datenbank in einen KDB-Cluster	Schreiben	kxDatabase*		
ResetUserPassword	Erteilt die Erlaubnis, das Passwort für einen FinSpace Benutzer zurückzusetzen	Schreiben	environment*		
			user*		
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren	environment		
			kxCluster		
			kxDatabase		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			kxDataview		
			kxEnvironment		
			kxScalingGroup		
			kxUser		
			kxVolume		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Tagging	environment		
			kxCluster		
			kxDatabase		
			kxDataview		
			kxEnvironment		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			kxScalingGroup		
			kxUser		
			kxVolume		
				aws:TagKeys	
UpdateEnvironment	Erteilt die Erlaubnis, eine FinSpace Umgebung zu aktualisieren	Schreiben	environment*		
UpdateKxClusterCodeConfiguration	Gewährt die Berechtigung zum Aktualisieren von Code-Konfigurationen für ein Cluster in einer verwalteten KDB-Umgebung	Schreiben	kxCluster*		
UpdateKxClusterDatabases	Gewährt die Berechtigung zum Aktualisieren von Datenbanken für ein Cluster in einer verwalteten KDB-Umgebung	Schreiben	kxCluster*		
UpdateKxDatabase	Gewährt die Berechtigung zum Aktualisieren einer KDB-Datenbank	Schreiben	kxDatabase*		
UpdateKxDataview	Gewährt die Berechtigung zum Aktualisieren einer Datenansicht in einer verwalteten kdb-Umgebung	Schreiben	kxDataview*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateKxEnvironment	Gewährt die Berechtigung zum Aktualisieren einer verwalteten KDB-Umgebung	Schreiben	kxEnvironment*		
UpdateKxEnvironmentNetwork	Gewährt die Berechtigung zum Aktualisieren des Netzwerks für eine verwaltete KDB-Umgebung	Schreiben	kxEnvironment*		
UpdateKxUser	Gewährt die Berechtigung zum Aktualisieren eines KDB-Benutzers	Schreiben	kxUser*		
UpdateKxVolume	Gewährt die Berechtigung zum Aktualisieren eines Volumes in einer verwalteten kdb-Umgebung	Schreiben	kxVolume*		
UpdateUser	Erteilt die Erlaubnis, einen FinSpace Benutzer zu aktualisieren	Schreiben	environment*		
			user*		

Von Amazon definierte Ressourcentypen FinSpace

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
environment	arn:${Partition}:finspace:${Region}:${Account}:environment/${EnvironmentId}	aws:ResourceTag/${TagKey}
user	arn:${Partition}:finspace:${Region}:${Account}:user/${UserId}	aws:ResourceTag/${TagKey}
kxEnvironment	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}	aws:ResourceTag/${TagKey}
kxUser	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxUser/${UserName}	aws:ResourceTag/${TagKey}
kxCluster	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxCluster/${KxCluster}	aws:ResourceTag/${TagKey}
kxDatabase	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxDatabase/${KxDatabase}	aws:ResourceTag/${TagKey}
kxScalingGroup	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxScalingGroup/${KxScalingGroup}	aws:ResourceTag/${TagKey}
kxDataview	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxDatabase/${KxDatabase}/kxDataview/${KxDataview}	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
kxVolume	`arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxVolume/${KxVolume}`	aws:ResourceTag/${TagKey}

Zustandsschlüssel für Amazon FinSpace

Amazon FinSpace definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	String
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüsselwertpaaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon FinSpace-API

Amazon FinSpace-API (Service-Präfix: `finspace-api`) bietet die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon FinSpace-API definierte Aktionen
- Von Amazon FinSpace-API definierte Ressourcentypen
- Bedingungsschlüssel für Amazon FinSpace-API

Von Amazon FinSpace-API definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetProgrammaticAccessCredentials	Gewährt die Berechtigung zum Abrufen von Anmeldeinformationen für den programmatischen Zugang zu FinSpace	Lesen	credential*		

Von Amazon FinSpace-API definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
credential	`arn:${Partition}:finspace-api:${Region}:${Account}:/credentials/programmatic`	

Bedingungsschlüssel für Amazon FinSpace-API

Die FinSpace-API besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Firewall Manager

AWS Firewall Manager (Servicepräfix: `fms`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungsschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Firewall Manager definierte Aktionen
- Von AWS Firewall Manager definierte Ressourcentypen
- Bedingungsschlüssel für AWS Firewall Manager

Von AWS Firewall Manager definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen.

Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateAdminAccount	Gewährt die Berechtigung, das AWS-Firewall-Manager-Administratorkonto festzulegen und aktiviert den Service in allen Organisationskonten	Schreiben			
AssociateThirdPartyFirewall	Gewährt die Berechtigung, den Firewall Manager-Administrator als Mandantenadministrator für den Firewall-Dienst eines Drittanbieters einzurichten	Schreiben			
BatchAssociateResource	Gewährt die Berechtigung zum Zuordnen von Ressourcen zu einem Ressourcensatz des AWS-Firewall-Managers	Schreiben	resource-set*		
BatchDisassociateResource	Gewährt die Berechtigung zum Trennen der Zuordnung von Ressourcen zu einem Ressourcensatz des AWS-Firewall-Managers	Schreiben	resource-set*		
DeleteAppsList	Gewährt die Berechtigung zum endgültigen Löschen einer AWS-Firewall-Manager-Anwendungsliste	Write	applications-list*		
DeleteNotificationChannel	Gewährt die Berechtigung zum Löschen einer AWS-Firewall-Manager-Zuordnung zur IAM-Rolle und zum	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Amazon Simple Notification Service (SNS)-Thema, mit dem der FM-Administrator über wesentliche FM-Ereignisse und -Fehler in der gesamten Organisation benachrichtigt wird				
DeletePolicy	Gewährt die Berechtigung zum endgültigen Löschen einer AWS-Firewall-Manager-Richtlinie	Write	policy*		
				aws:ResourceTag/${TagKey}	
DeleteProtocolsList	Gewährt die Berechtigung zum endgültigen Löschen einer AWS-Firewall-Manager-Protokollliste	Schreiben	protocols-list*		
DeleteResourceSet	Gewährt die Berechtigung zum endgültigen Löschen eines AWS-Firewall-Manager-Ressourcensatzes	Schreiben	resource-set*		
				aws:ResourceTag/${TagKey}	
DisassociateAdminAccount	Gewährt die Berechtigung, die Zuordnung des Kontos aufzuheben, das als AWS-Firewall-Manager-Administratorkonto festgelegt wurde, und deaktiviert den Service in allen Organisationskonten	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateThirdPartyFirewall	Gewährt die Berechtigung, einen Firewall Manager-Administrator von einem Mandanten mit Drittanbieter-Firewall zu entfernen	Schreiben			
GetAdminAccount	Gewährt die Berechtigung, das AWS-Organizations-Konto zurückzugeben, das AWS Firewall Manager als AWS-Firewall-Manager-Administrator zugeordnet ist	Lesen			
GetAdminScope	Gewährt die Berechtigung zum Zurückgeben von Informationen über den Verwaltungsbereich des angegebenen Kontos	Lesen			
GetAppsList	Gewährt die Berechtigung, Informationen zur angegebenen AWS-Firewall-Manager-Anwendungsliste zurückzugeben	Read	applications-list*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetComplianceDetail	Gewährt die Berechtigung, detaillierte Compliance-Informationen zum angegebenen Mitgliedskonto abzurufen. Zu den Details gehören Ressourcen, die die angegebene Richtlinie erfüllen oder nicht erfüllen.	Read	policy*		
GetNotificationChannel	Gewährt die Berechtigung, Informationen zum Amazon Simple Notification Service (SNS)-Thema zurückzugeben, das zum Aufzeichnen der AWS-Firewall-Manager-SNS-Protokolle verwendet wird	Read			
GetPolicy	Gewährt die Berechtigung, Informationen zur angegebenen AWS-Firewall-Manager-Richtlinie zurückzugeben	Read	policy*		
GetProtectionStatus	Gewährt die Berechtigung, im Falle eines potenziellen DDoS-Angriffs zusammenfassende Informationen auf Richtlinienebene zurückzugeben	Read	policy*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetProtocolsList	Gewährt die Berechtigung, Informationen zur angegebenen Liste von AWS-Firewall-Manager-Protokollen zurückzugeben	Lesen	protocols-list*		
GetResourceSet	Gewährt die Berechtigung zum Zurückgeben von Informationen über den angegebenen AWS-Firewall-Manager-Ressourcensatz	Lesen	resource-set*		
GetThirdPartyFirewallAssociationStatus	Gewährt einem Anbieterm andanten mit Drittanbieter-Firewall die Berechtigung zum Abrufen des Onboarding-Status eines Firewall Manager-Administratorkontos	Lesen			
GetViolationDetails	Gewährt die Berechtigung, Verstöße für eine Ressource auf der Grundlage der angegebenen AWS-Firewall-Manager-Richtlinie und dem AWS-Konto abzurufen	Lesen	policy*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAdminAccountsForOrganization	Gewährt die Berechtigung zum Zurückgeben eines AdminAccounts-Objekts, das die Firewall-Manager-Administratoren innerhalb der Organisation auflistet, die durch AssociateAdminAccount in den Firewall Manager eingebunden sind	Auflisten			
ListAdminsManagingAccount	Gewährt die Berechtigung zum Auflisten der Konten, die das angegebene Mitgliedskonto von AWS-Organisationen verwalten	Auflisten			
ListAppsLists	Gewährt die Berechtigung, ein Array von AppsListDataSummary-Objekten zurückzugeben	List			
ListComplianceStatus	Gewährt die Berechtigung, ein Array von PolicyComplianceStatus-Objekten in der Antwort abzurufen. Mit PolicyComplianceStatus erhalten Sie eine Übersicht der Mitgliedskonten, die durch die angegebene Richtlinie geschützt sind.	Auflisten	policy*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDiscoveredResources	Gewährt die Berechtigung zum Abrufen eines Arrays von Ressourcen in den Konten der Organisation, die einem Ressourcensatz zugeordnet werden können	Auflisten			
ListMemberAccounts	Gewährt die Berechtigung, ein Array von Mitgliedskonto-IDs abzurufen, wenn der Aufrufer ein FMS-Administratorkonto ist	List			
ListPolicies	Gewährt die Berechtigung, ein Array von PolicySummary-Objekten in der Antwort abzurufen	List			
ListProtocolsLists	Gewährt die Berechtigung, ein Array von ProtocolsListDataSummary-Objekten zurückzugeben	Auflisten			
ListResourceSetResources	Gewährt die Berechtigung zum Abrufen eines Arrays von Ressourcen, die mit Ihnen verknüpft sind	Auflisten	resource-set*		
ListResourceSets	Gewährt die Berechtigung zum Abrufen eines Arrays von ResourceSetSummary-Objekten	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen	policy*		
ListThirdPartyFirewallFirewallPolicies	Gewährt die Berechtigung zum Abrufen einer Liste aller Drittanbieter-Firewall-Richtlinien, die dem Konto des Administrators der Drittanbieter-Firewall zugewiesen sind	Auflisten			
PutAdminAccount	Gewährt die Berechtigung zum Erstellen oder Aktualisieren eines Firewall-Manager-Administratorkontos	Schreiben			
PutAppsList	Gewährt die Berechtigung zum Erstellen einer AWS-Firewall-Manager-Anwendungsliste	Write	applications-list*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutNotificationChannel	Gewährt die Berechtigung, die IAM-Rolle und das Amazon-Simple-Notification-Service(SNS)-Thema zu bezeichnen, die von AWS Firewall Manager (FM) verwendet werden können, um den FM-Administrator über wesentliche FM-Ereignisse und -Fehler in der gesamten Organisation zu benachrichtigen	Write			
PutPolicy	Gewährt die Berechtigung zum Erstellen einer AWS-Firewall-Manager-Richtlinie	Write	policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutProtocolsList	Gewährt die Berechtigung zum Erstellen einer AWS-Firewall-Manager-Protokollliste.	Schreiben	protocols-list*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutResourceSet	Gewährt die Berechtigung zum Erstellen eines AWS-Firewall-Manager-Ressourcensatzes	Schreiben	resource-set*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Gewährt die Berechtigung zum Hinzufügen eines Tags zu einer bestimmten Ressource	Markieren	applications-list		
			policy		
			protocols-list		
			resource-set		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen eines Tags von einer bestimmten Ressource	Markieren	applications-list		
			policy		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			protocols-list		
			resource-set		
				aws:TagKeys	

Von AWS Firewall Manager definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
policy	`arn:${Partition}:fms:${Region}:${Account}:policy/${Id}`	aws:ResourceTag/${TagKey}
applications-list	`arn:${Partition}:fms:${Region}:${Account}:applications-list/${Id}`	aws:ResourceTag/${TagKey}
protocols-list	`arn:${Partition}:fms:${Region}:${Account}:protocols-list/${Id}`	aws:ResourceTag/${TagKey}
resource-set	`arn:${Partition}:fms:${Region}:${Account}:resource-set/${Id}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Firewall Manager

AWS Firewall Manager definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüsselwertpaaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Forecast

Amazon Forecast (Servicepräfix: `forecast`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Forecast definierte Aktionen

- Von Amazon Forecast definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Forecast

Von Amazon Forecast definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAutoPredictor	Gewährt die Berechtigung zum Erstellen eines Auto-Prädiktors	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataset	Gewährt die Berechtigung zum Erstellen eines Dataset	Write	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDatasetGroup	Gewährt die Berechtigung zum Erstellen einer Dataset-Gruppe	Write	datasetGroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDatasetImportJob	Gewährt die Berechtigung zum Erstellen einer Dataset-Importaufgabe	Schreiben	datasetImportJob*		
				aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
CreateExplainability	Gewährt die Berechtigung zum Erstellen einer Erklärbarkeit	Schreiben	forecast*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExplainabilityExport	Gewährt die Berechtigung zum Erstellen eines Erklärbarkeitsexports mit einer Erklärbarkeitsressource	Schreiben	explainability*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateForecast	Gewährt die Berechtigung zum Erstellen einer Prognose	Schreiben	predictor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateForecastEndpoint [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines Endpunkts mit einer Predictor-Ressource	Schreiben	predictor*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateForecastExportJob	Gewährt die Berechtigung zum Erstellen einer Prognose-Exportaufgabe mit einer Prognoseressource	Schreiben	forecast*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMonitor	Gewährt die Berechtigung zum Erstellen einer Überprüfung mit einer Predictor-Ressource	Schreiben	predictor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePredictor	Gewährt die Berechtigung zum Erstellen eines Prädiktors	Write	datasetGroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreatePredictorBacktestExportJob	Gewährt die Berechtigung zum Erstellen einer Prädiktor-Backtest-Exportaufgabe mit einem Prädiktor	Schreiben	predictor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWhatIfAnalysis	Gewährt die Berechtigung zum Erstellen einer Was-wäre-wenn-Analyse	Schreiben	forecast*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWhatIfForecast	Gewährt die Berechtigung zum Erstellen einer Was-wäre-wenn-Prognose	Schreiben	whatIfAnalysis*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWhatIfForecastExport	Gewährt die Berechtigung zum Erstellen eines Was-wäre-wenn-Prognose-Exports mit Was-wäre-wenn-Prognoseressourcen	Schreiben	whatIfForecast*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDataset	Gewährt die Berechtigung zum Löschen eines Dataset	Write	dataset*		
DeleteDatasetGroup	Gewährt die Berechtigung zum Löschen einer Dataset-Gruppe	Write	datasetGroup*		
DeleteDatasetImportJob	Gewährt die Berechtigung zum Löschen einer Dataset-Importaufgabe	Schreiben	datasetImportJob*		
DeleteExplainability	Gewährt die Berechtigung zum Löschen einer Erklärbarkeit	Schreiben	explainability*		
DeleteExplainabilityExport	Gewährt die Berechtigung zum Löschen eines Erklärbarkeitsexports	Schreiben	explainabilityExport*		
DeleteForecast	Gewährt die Berechtigung zum Löschen einer Prognose	Schreiben	forecast*		
DeleteForecastEndpoint [nur Berechtigung]	Gewährt die Berechtigung zum Löschen einer Endpunktressource	Schreiben	endpoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteForecastExportJob	Gewährt die Berechtigung zum Löschen einer Prognose-Exportaufgabe	Schreiben	forecastExport*		
DeleteMonitor	Gewährt die Berechtigung zum Löschen einer Überprüfungs-Ressource	Schreiben	monitor*		
DeletePredictor	Gewährt die Berechtigung zum Löschen eines Prädiktors	Write	predictor*		
DeletePredictorBacktestExportJob	Gewährt die Berechtigung zum Löschen einer Prädiktor-Backtest-Exportaufgabe	Write	predictorBacktestExportJob*		
DeleteResourceTree	Gewährt die Berechtigung zum Löschen einer Ressource und ihrer untergeordneten Ressourcen	Schreiben	dataset*		
			datasetGroup*		
			datasetImportJob*		
			endpoint*		
			explainability*		
			explainabilityExport*		
			forecast*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			forecastExport*		
			monitor*		
			predictor*		
			predictorBacktestExportJob*		
			whatIfAnalysis*		
			whatIfForecast*		
			whatIfForecastExport*		
DeleteWhatIfAnalysis	Gewährt die Berechtigung zum Löschen einer Was-wäre-wenn-Analyse	Schreiben	whatIfAnalysis*		
DeleteWhatIfForecast	Gewährt die Berechtigung zum Löschen einer Was-wäre-wenn-Prognose	Schreiben	whatIfForecast*		
DeleteWhatIfForecastExport	Gewährt die Berechtigung zum Löschen eines Was-wäre-wenn-Prognoseexports	Schreiben	whatIfForecastExport*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeAutoPredictor	Gewährt die Berechtigung zum Beschreiben eines Auto-Prädiktors	Lesen	predictor*		
DescribeDataset	Gewährt die Berechtigung zum Beschreiben eines Dataset	Read	dataset*		
DescribeDatasetGroup	Gewährt die Berechtigung zum Beschreiben einer Dataset-Gruppe	Read	datasetGroup*		
DescribeDatasetImportJob	Gewährt die Berechtigung zum Beschreiben einer Dataset-Importaufgabe	Lesen	datasetImportJob*		
DescribeExplainability	Gewährt die Berechtigung zum Beschreiben einer Erklärbarkeit	Lesen	explainability*		
DescribeExplainabilityExport	Gewährt die Berechtigung zum Beschreiben eines Erklärbarkeitsexports	Lesen	explainabilityExport*		
DescribeForecast	Gewährt die Berechtigung zum Beschreiben einer Prognose	Lesen	forecast*		
DescribeForecastEndpoint [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben einer Endpunktressource	Lesen	endpoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeForecastExportJob	Gewährt die Berechtigung zum Beschreiben einer Prognose-Exportaufgabe	Lesen	forecastExport*		
DescribeMonitor	Gewährt die Berechtigung zum Beschreiben einer Überprüfungs-Ressource	Lesen	monitor*		
DescribePredictor	Gewährt die Berechtigung zum Beschreiben eines Prädiktors	Read	predictor*		
DescribePredictorBacktestExportJob	Gewährt die Berechtigung zum Beschreiben einer Prädiktor-Backtest-Exportaufgabe	Lesen	predictorBacktestExportJob*		
DescribeWhatIfAnalysis	Gewährt die Berechtigung zum Beschreiben einer Was-wäre-wenn-Analyse	Lesen	whatIfAnalysis*		
DescribeWhatIfForecast	Gewährt die Berechtigung zum Beschreiben einer Was-wäre-wenn-Prognose	Lesen	whatIfForecast*		
DescribeWhatIfForecastExport	Gewährt die Berechtigung zum Beschreiben eines Was-wäre-wenn-Prognoseexports	Lesen	whatIfForecastExport*		
GetAccuracyMetrics	Gewährt die Berechtigung zum Abrufen der Genauigkeitsmetriken für einen Prädiktor	Lesen	predictor*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetRecentForecastContext [nur Berechtigung]	Erteilt die Berechtigung zum Abrufen des Prognosekontexts einer Zeitreihe für einen Endpunkt	Lesen	endpoint*		
InvokeForecastEndpoint [nur Berechtigung]	Erteilt die Berechtigung zum Aufrufen des Endpunkts, um eine Prognose für eine Zeitreihe abzurufen	Lesen	endpoint*		
ListDatasetGroups	Gewährt die Berechtigung zum Auflisten aller Dataset-Gruppen	Lesen			
ListDatasetImportJobs	Gewährt die Berechtigung zum Auflisten aller Dataset-Importaufgaben	Lesen			
ListDatasets	Gewährt die Berechtigung zum Auflisten aller Datasets	Lesen			
ListExplainabilities	Gewährt die Berechtigung zum Auflisten aller Erklärbarkeiten	Lesen			
ListExplainabilityExports	Gewährt die Berechtigung zum Auflisten aller Erklärbarkeitexporte	Lesen			
ListForecastExportJobs	Gewährt die Berechtigung zum Auflisten aller Prognose-Exportaufgaben	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListForecasts	Gewährt die Berechtigung zum Auflisten aller Prognosen	Lesen			
ListMonitorEvaluations	Gewährt die Berechtigung zum Auflisten des gesamten Überprüfungsauswertergebnisses für eine Überprüfung	Lesen	monitor*		
ListMonitors	Gewährt die Berechtigung zum Auflisten aller Überprüfungs-Ressourcen	Lesen			
ListPredictorBacktestExportJobs	Gewährt die Berechtigung zum Auflisten aller Prädiktor-Backtest-Exportaufgaben	Lesen			
ListPredictors	Gewährt die Berechtigung zum Auflisten aller Prädiktoren	Lesen			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für eine Amazon Forecast-Ressource	Lesen	dataset		
			datasetGroup		
			datasetImportJob		
			endpoint		
			explainability		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			explainabilityExport		
			forecast		
			forecastExport		
			monitor		
			predictor		
			predictorBacktestExportJob		
			whatIfAnalysis		
			whatIfForecast		
			whatIfForecastExport		
ListWhatIfAnalyses	Gewährt die Berechtigung zum Auflisten aller Was-wäre-wenn-Analysen	Lesen			
ListWhatIfForecastExports	Gewährt die Berechtigung zum Auflisten aller Was-wäre-wenn-Prognoseexports	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListWhatIfForecasts	Gewährt die Berechtigung zum Auflisten aller Was-wäre-wenn-Prognosen	Lesen			
QueryForecast	Gewährt die Berechtigung zum Abrufen einer Prognose für ein einzelnes Element	Lesen	forecast*		
QueryWhatIfForecast	Gewährt die Berechtigung zum Abrufen einer Was-wäre-wenn-Prognose für ein einzelnes Element	Lesen	whatIfForecast*		
ResumeResource	Gewährt die Berechtigung zur Wiederaufnahme von Amazon-Forecast-Ressourcenaufgaben	Schreiben	monitor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StopResource	Gewährt die Berechtigung zum Anhalten von Amazon Forecast-Ressourcenaufgaben	Write	datasetImportJob*		
			endpoint*		
			explainability*		
			explainabilityExport*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			forecast*		
			forecastExport*		
			monitor*		
			predictor*		
			predictorBacktestExportJob*		
			whatIfAnalysis*		
			whatIfForecast*		
			whatIfForecastExport*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Gewährt die Berechtigung, die angegebenen Tags einer Ressource zuzuordnen	Markieren	dataset		
			datasetGroup		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			datasetImportJob		
			endpoint		
			explainability		
			explainabilityExport		
			forecast		
			forecastExport		
			monitor		
			predictor		
			predictorBacktestExportJob		
			whatIfAnalysis		
			whatIfForecast		
			whatIfForecastExport		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Löschen der angegebenen Tags für eine Ressource	Markieren	dataset		
			datasetGroup		
			datasetImportJob		
			endpoint		
			explainability		
			explainabilityExport		
			forecast		
			forecastExport		
			monitor		
			predictor		
			predictorBacktestExportJob		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			whatIfAnalysis		
			whatIfForecast		
			whatIfForecastExport		
				aws:TagKeys	
UpdateDatasetGroup	Gewährt die Berechtigung zum Aktualisieren einer Dataset-Gruppe	Write	dataset*		
			datasetGroup*		

Von Amazon Forecast definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
dataset	`arn:${Partition}:forecast:${Region}:${Account}:dataset/${ResourceId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
datasetGroup	arn:${Partition}:forecast:${Region}:${Account}:dataset-group/${ResourceId}	aws:ResourceTag/${TagKey}
datasetImportJob	arn:${Partition}:forecast:${Region}:${Account}:dataset-import-job/${ResourceId}	aws:ResourceTag/${TagKey}
algorithm	arn:${Partition}:forecast:::algorithm/${ResourceId}	
predictor	arn:${Partition}:forecast:${Region}:${Account}:predictor/${ResourceId}	aws:ResourceTag/${TagKey}
predictorBacktestExportJob	arn:${Partition}:forecast:${Region}:${Account}:predictor-backtest-export-job/${ResourceId}	aws:ResourceTag/${TagKey}
forecast	arn:${Partition}:forecast:${Region}:${Account}:forecast/${ResourceId}	aws:ResourceTag/${TagKey}
forecastExport	arn:${Partition}:forecast:${Region}:${Account}:forecast-export-job/${ResourceId}	aws:ResourceTag/${TagKey}
explainability	arn:${Partition}:forecast:${Region}:${Account}:explainability/${ResourceId}	aws:ResourceTag/${TagKey}
explainabilityExport	arn:${Partition}:forecast:${Region}:${Account}:explainability-export/${ResourceId}	aws:ResourceTag/${TagKey}
monitor	arn:${Partition}:forecast:${Region}:${Account}:monitor/${ResourceId}	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
whatIfAnalysis	`arn:${Partition}:forecast:${Region}:${Account}:what-if-analysis/${ResourceId}`	aws:ResourceTag/${TagKey}
whatIfForecast	`arn:${Partition}:forecast:${Region}:${Account}:what-if-forecast/${ResourceId}`	aws:ResourceTag/${TagKey}
whatIfForecastExport	`arn:${Partition}:forecast:${Region}:${Account}:what-if-forecast-export/${ResourceId}`	aws:ResourceTag/${TagKey}
endpoint	`arn:${Partition}:forecast:${Region}:${Account}:forecast-endpoint/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Forecast

Amazon Forecast definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Fraud Detector

Amazon Fraud Detector (Servicepräfix: `frauddetector`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Fraud Detector definierte Aktionen
- Vom Amazon Fraud Detector definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Fraud Detector

Von Amazon Fraud Detector definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchCreateVariable	Gewährt die Berechtigung zum Erstellen eines Batches von Variablen	Write		aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
BatchGetVariable	Gewährt die Berechtigung zum Abrufen eines Batches von Variablen	Auflisten	variable*		
CancelBatchImportJob	Gewährt die Berechtigung zum Abbrechen des angegebenen Batch-Importauftrags	Schreiben	batch-import*		
CancelBatchPredictionJob	Gewährt die Berechtigung zum Abbrechen des angegebenen Batch-Vorhersageauftrags	Schreiben	batch-prediction*		
CreateBatchImportJob	Gewährt die Berechtigung zum Erstellen einer Batch-Import-Aufgabe	Schreiben	batch-import*		
			event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBatchPredictionJob	Gewährt die Berechtigung zum Erstellen eines Batch-Vorhersageauftrags	Write	batch-prediction*		
			detector*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			detector-version*		
			event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDetectorVersion	Gewährt die Berechtigung zum Erstellen einer Detektorversion. Die Detektorversion startet in einem DRAFT-Status.	Schreiben	detector*		
			external-model		
			model-version		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateList	Gewährt die Berechtigung zum Erstellen einer Liste	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateModel	Gewährt die Berechtigung zum Erstellen eines Modells mit dem angegebenen Modelltyp	Write	event-type*		
			model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelVersion	Gewährt die Berechtigung zum Erstellen einer Version des Modells mit dem angegebenen Modelltyp und der Modell-ID	Write	model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRule	Gewährt die Berechtigung zum Erstellen einer Regel zur Verwendung mit dem angegebenen Detektor	Write	detector*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateVariable	Gewährt die Berechtigung zum Erstellen einer Variablen	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBatchImportJob	Gewährt die Berechtigung zum Löschen einer Batch-Import-Aufgabe	Schreiben	batch-import*		
DeleteBatchPredictionJob	Gewährt die Berechtigung zum Löschen eines Batch-Vorhersageauftrags	Write	batch-prediction*		
DeleteDetector	Gewährt die Berechtigung zum Löschen des Detektors. Bevor Sie einen Detektor löschen, müssen Sie zuerst alle Detektorversionen und Regelversionen löschen, die dem Detektor zugeordnet sind.	Write	detector*		
DeleteDetectorVersion	Gewährt die Berechtigung zum Löschen der Detektorversion. Sie können keine Detektorversionen löschen, die sich im Status ACTIVE befinden.	Write	detector-version*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteEntityType	Gewährt die Berechtigung zum Löschen eines Entitätstypen Sie können keinen Entitätstyp löschen, der in einem Ereignistyp enthalten ist.	Write	entity-type*		
DeleteEvent	Gewährt die Berechtigung zum Löschen des angegebenen Ereignisses	Write	event-type*		
DeleteEventType	Gewährt die Berechtigung zum Löschen eines Ereignistyps. Sie können keinen Ereignistyp löschen, der in einem Detektor oder einem Modell verwendet wird.	Schreiben	event-type*		
DeleteEventsByEventType	Gewährt die Berechtigung zum Löschen von Ereignissen des angegebenen Ereignistyps	Schreiben	event-type*		
DeleteExternalModel	Gewährt die Berechtigung zum Entfernen des SageMaker-Modells aus Amazon Fraud Detector. Sie können ein Amazon SageMaker-Modell entfernen, wenn es nicht mit einer Detektorversion verknüpft ist.	Write	external-model*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteLabel	Gewährt die Berechtigung zum Löschen einer Bezeichnung. Sie können keine Labels löschen, die in einem Ereignistyp in Amazon Fraud Detector enthalten sind. Sie können ein Label nicht löschen, das einer Ereignis-ID zugewiesen ist. Sie müssen zuerst die entsprechende Ereignis-ID löschen.	Schreiben	label*		
DeleteList	Gewährt die Berechtigung zum Löschen einer Liste	Schreiben	list*		
				aws:ResourceTag/${TagKey}	
DeleteModel	Gewährt die Berechtigung zum Löschen eines Modells. Sie können Modelle und Modellversionen in Amazon Fraud Detector löschen, sofern sie nicht mit einer Detektorversion verknüpft sind.	Write	model*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteModelVersion	Gewährt die Berechtigung zum Löschen einer Modellversion. Sie können Modelle und Modellversionen in Amazon Fraud Detector löschen, sofern sie nicht mit einer Detektorversion verknüpft sind.	Write	model-version*		
DeleteOutcome	Gewährt die Berechtigung zum Löschen eines Ergebnisses. Sie können kein Ergebnis löschen, das in einer Regelversion verwendet wird.	Write	outcome*		
DeleteRule	Gewährt die Berechtigung zum Löschen der Regel. Sie können eine Regelversion nicht löschen, wenn sie von einer AKTIVEN oder INAKTIVEN Detektorversion verwendet wird.	Write	rule*		
DeleteVariable	Gewährt die Berechtigung zum Löschen einer Variablen. Sie können keine Variablen löschen, die in einem Ereignistyp in Amazon Fraud Detector enthalten sind.	Write	variable*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDetector	Gewährt die Berechtigung zum Abrufen aller Versionen für einen bestimmten Detektor	Read	detector*		
DescribeModelVersions	Gewährt die Berechtigung zum Abrufen aller Modellversionen für den angegebenen Modelltyp oder für den angegebenen Modelltyp und die Modell-ID. Sie können auch Details für eine einzelne, angegebene Modellversion abrufen.	Lesen	model-version		
GetBatchImportJobValidationReport [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen des Datenvalidierungsberichts für einen bestimmten Stapelimportauftrags	Lesen	batch-import*		
GetBatchImportJobs	Gewährt die Berechtigung zum Abrufen aller Batch-Import-Aufträge oder eines bestimmten Auftrags, wenn Sie eine Auftrags-ID angeben	Auflisten	batch-import		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBatchPredictionJobs	Gewährt die Berechtigung zum Abrufen aller Batchvorhersage-Aufträge oder eines bestimmten Auftrags, wenn Sie eine Auftrags-ID angeben. Dies ist eine paginierte API. Wenn Sie für MaxResults null angeben, ruft diese Aktion maximal 50 Datensätze pro Seite ab. Wenn Sie einen Wert für MaxResults angeben, muss dieser zwischen 1 und 50 liegen. Um die Ergebnisse der nächsten Seite zu erhalten, geben Sie das Paginierungstoken aus der GetBatchPredictionJobsResponse als Teil Ihrer Anforderung an. Ein Null-Paginierungs-Token ruf die Datensätze von Anfang an ab.	Auflisten	batch-prediction		
GetDeleteEventsByEventTypeStatus	Gewährt die Berechtigung zum Abrufen eines bestimmten Ereignistyps-DeleteEventsByEventType-API-Ausführungsstatus	Lesen	event-type*		
GetDetectorVersion	Gewährt die Berechtigung zum Abrufen einer bestimmten Detektorversion	Lesen	detector-version*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDetectors	Gewährt die Berechtigung zum Abrufen aller Detektoren oder eines einzelnen Detektors, wenn eine DetectorID angegeben ist. Dies ist eine paginierte API. Wenn Sie für MaxResults null angeben, ruft diese Aktion maximal 10 Datensätze pro Seite ab. Wenn Sie einen Wert für MaxResults angeben, muss dieser zwischen 5 und 10 liegen. Um die Ergebnisse der nächsten Seite zu erhalten, geben Sie das Paginierungstoken aus der GetDetectorsRespons als Teil Ihrer Anforderung an. Ein Null-Paginierungs-Token ruf die Datensätze von Anfang an ab.	List	detector		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetEntityTypes	Gewährt die Berechtigung zum Abrufen aller Entitätstypen oder eines bestimmten Entitätstyps, wenn ein Name angegeben wird. Dies ist eine paginierte API. Wenn Sie für MaxResults null angeben, ruft diese Aktion maximal 10 Datensätze pro Seite ab. Wenn Sie einen Wert für MaxResults angeben, muss dieser zwischen 5 und 10 liegen. Um die Ergebnisse der nächsten Seite zu erhalten, geben Sie das Paginierungstoken aus der GetEntityTypesResponse als Teil Ihrer Anforderung an. Ein Null-Paginierungs-Token ruf die Datensätze von Anfang an ab.	Auflisten	entity-type		
GetEvent	Gewährt die Berechtigung zum Abrufen der Details des angegebenen Ereignisses	Lesen	event-type*		
GetEventPrediction	Gewährt die Berechtigung zur Auswertung eines Ereignisses gegen eine Detektorversion. Wenn keine Versions-ID angegeben wird, wird die Version des Detektors (ACTIVE) verwendet.	Lesen	detector*		
			detector-version*		
			event-type*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetEventPrediction Metadata	Gewährt die Berechtigung, weitere Details zu einer bestimmten Vorhersage zu erhalten	Lesen	detector*		
			detector-version*		
			event-type*		
GetEventTypes	Gewährt die Berechtigung zum Abrufen aller Ereignistypen oder eines bestimmten Ereignistyps, wenn der Name angegeben wird. Dies ist eine paginierte API. Wenn Sie für MaxResults null angeben, ruft diese Aktion maximal 10 Datensätze pro Seite ab. Wenn Sie einen Wert für MaxResults angeben, muss dieser zwischen 5 und 10 liegen. Um die Ergebnisse der nächsten Seite zu erhalten, geben Sie das Paginierungs-Token aus der GetEventTypesResponse als Teil Ihrer Anforderung an. Ein Null-Paginierungs-Token ruf die Datensätze von Anfang an ab.	List	event-type		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetExternalModels	Gewährt die Berechtigung zum Abrufen der Details für ein oder mehrere Amazon SageMaker-Modelle, die in den Service importiert wurden. Dies ist eine paginierte API. Wenn Sie für maxResults null angeben, ruft diese Aktion maximal 10 Datensätze pro Seite ab. Wenn Sie einen Wert für MaxResults angeben, muss dieser zwischen 5 und 10 liegen. Um die Ergebnisse der nächsten Seite zu erhalten, stellen Sie das Paginierungs-Token aus dem GetExternalModelsResult als Teil Ihrer Anforderung bereit. Ein Null-Paginierungs-Token ruf die Datensätze von Anfang an ab.	List	external-model		
GetKMSEncryptionKey	Gewährt die Berechtigung zum Abrufen der Verschlüsselungsschlüssel, wenn ein KMS-Kundenmasterschlüssel (Key Management Service) angegeben wurde, der zum Verschlüsseln von Inhalten in Amazon Fraud Detector verwendet werden soll.	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetLabels	Gewährt die Berechtigung zum Abrufen aller Labels oder eines bestimmten Label, wenn der Name angegeben wird. Dies ist eine paginierte API. Wenn Sie für MaxResults null angeben, ruft diese Aktion maximal 50 Datensätze pro Seite ab. Wenn Sie einen Wert für MaxResults angeben, muss dieser zwischen 10 und 50 liegen. Um die Ergebnisse der nächsten Seite zu erhalten, geben Sie das Paginierungstoken aus der GetGetLabelsResponse als Teil Ihrer Anforderung an. Ein Null-Paginierungs-Token ruf die Datensätze von Anfang an ab.	Auflisten	label		
GetListElements	Gewährt die Berechtigung zum Abrufen von Elementen einer Liste	Lesen	list*		
				aws:ResourceTag/${TagKey}	
GetListsMetadata	Gewährt die Berechtigung zum Abrufen von Metadaten über Listen	Auflisten	list		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetModelVersion	Gewährt die Berechtigung zum Abrufen der Details der angegebenen Modellversion	Lesen	model-version*		
GetModels	Gewährt die Berechtigung zum Abrufen eines oder mehrerer Modelle. Ruft alle Modelle für das AWS-Konto ab, wenn kein Modelltyp und keine Modell-ID angegeben sind Ruft alle Modelle für das AWS-Konto und den Modelltyp ab, wenn der Modelltyp angegeben ist, die Modell-ID jedoch nicht angegeben wird Ruft ein bestimmtes Modell ab, wenn (Modelltyp, Modell-ID)-Tupel angegeben ist.	List	model		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetOutcomes	Gewährt die Berechtigung zum Abrufen eines oder mehrerer Ergebnisse. Dies ist eine paginierte API. Wenn Sie für maxResults null angeben, ruft diese Aktion maximal 100 Datensätze pro Seite ab. Wenn Sie einen Wert für MaxResults angeben, muss dieser zwischen 50 und 100 liegen. Um die Ergebnisse der nächsten Seite abzurufen, stellen Sie das Paginierungs-Token aus dem GetOutcomesResult als Teil der Anforderung bereit. Ein Null-Paginierungs-Token ruf die Datensätze von Anfang an ab.	List	outcome		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetRules	Gewährt die Berechtigung zum Abrufen aller Regeln für einen Detektor (paginiert), wenn RuleId und RuleVersion nicht angegeben sind. Ruft alle Regeln für den Detektor und die RuleID ab, falls vorhanden (paginiert). Ruft eine bestimmte Regel ab, wenn sowohl die RuleID als auch die RuleVersion angegeben sind.	List	rule		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetVariables	Gewährt die Berechtigung zum Abrufen aller Variablen oder der spezifischen Variable. Dies ist eine paginierte API. Die Angabe von maxSizePerPage mit Null führt zum Abrufen von maximal 100 Datensätzen pro Seite. Wenn Sie maxSizePerPage angeben, muss der Wert zwischen 50 und 100 liegen. Um das Ergebnis der nächsten Seite zu erhalten, geben Sie ein Paginierungs-Token von GetVariablesResult als Teil Ihrer Anfrage an. Das Null-Paginierungs-Token ruf die Datensätze von Anfang an ab.	Auflisten	variable		
ListEventPredictions	Gewährt die Berechtigung, eine Liste vergangener Vorhersagen zu erhalten	Auflisten	detector		
			detector-version		
			event-type		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Auflisten aller mit der Ressource verknüpften Tags. Dies ist eine paginierte API. Um die Ergebnisse der nächsten Seite zu erhalten, geben Sie das Paginierungstoken aus der Antwort als Teil Ihrer Anforderung an. Ein Null-Paginierungs-Token ruft die Datensätze von Anfang an ab.	Lesen	batch-import		
			batch-prediction		
			detector		
			detector-version		
			entity-type		
			event-type		
			external-model		
			label		
			list		
			model		
			model-version		
			outcome		
			rule		
			variable		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutDetector	Gewährt die Berechtigung zum Erstellen oder Aktualisieren eines Detektors	Write	detector*		
			event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutEntityType	Gewährt die Berechtigung zum Erstellen oder Aktualisieren eines Entitätstyps. Eine Entität stellt dar, wer das Ereignis ausführt. Sie übergeben im Rahmen einer Betrugsprognose die Entitäts-ID, um die spezifische Entität anzugeben, die das Ereignis ausgeführt hat. Ein Entitätstyp klassifiziert die Entität. Zu den Beispielklassifizierungen gehören Kunden, Händler oder Konto.	Write	entity-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutEventType	Gewährt die Berechtigung zum Erstellen oder Aktualisieren eines Ereignistyps. Ein Ereignis ist eine geschäftliche Aktivität, die auf Betrugsrisiken überprüft wird. Mit Amazon Fraud Detector generieren Sie Betrugsprognosen für Ereignisse. Ein Ereignistyp definiert die Struktur für ein Ereignis, das an Amazon Fraud Detector gesendet wird. Dazu gehören die Variablen, die als Teil des Ereignisses gesendet werden, die Entität, die das Ereignis ausführt (z. B. ein Kunde), und die Beschriftungen, die das Ereignis klassifizieren. Beispiel für Ereignistypen sind etwa Online-Zahlungstransaktionen, Kontoregistrierungen und Authentifizierungen.	Write	event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutExternalModel	Gewährt die Berechtigung zum Erstellen oder Aktualisieren eines Amazon SageMaker-Modellendpunkts. Sie können diese Aktion auch dazu verwenden, die Konfiguration des Modellendpunkts zu aktualisieren, einschließlich der IAM-Rolle und/oder der zugeordneten Variablen.	Write	event-type*		
			external-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutKMSEncryptionKey	Gewährt die Berechtigung zum Angeben des KMS (Key Management Service)-Customer Master Key (CMK), der zum Verschlüsseln von Inhalten in Amazon Fraud Detector verwendet werden soll.	Write			
PutLabel	Gewährt die Berechtigung zum Erstellen oder Aktualisieren einer Bezeichnung. Eine Beschriftung klassifiziert ein Ereignis als betrügerisch oder legitim. Beschriftungen werden Ereignistypen zugeordnet und verwendet, um überwachte Machine Learning-Modelle in Amazon Fraud Detector zu trainieren.	Write	label*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutOutcome	Gewährt die Berechtigung zum Erstellen oder Aktualisieren eines Ergebnisses	Schreiben	outcome*		
				aws:RequestTag/${TagKey} aws:TagKeys	
SendEvent	Gewährt die Berechtigung zum Senden eines Ereignisses	Schreiben	event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Gewährt die Berechtigung zum Anfügen von Tags an eine Ressource	Markieren	batch-import		
			batch-prediction		
			detector		
			detector-version		
			entity-type		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			event-type		
			external-model		
			label		
			list		
			model		
			model-version		
			outcome		
			rule		
			variable		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Ressource	Markieren	batch-import		
			batch-prediction		
			detector		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			detector-version		
			entity-type		
			event-type		
			external-model		
			label		
			list		
			model		
			model-version		
			outcome		
			rule		
			variable		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateDetectorVersion	Gewährt die Berechtigung zum Aktualisieren einer Detektorversion. Zu den Detektorversionsattributen, die Sie aktualisieren können, gehören Modelle, externe Modellendpunkte, Regeln und Beschreibungen. Sie können nur eine DRAFT-Detektorversion aktualisieren.	Write	detector*		
			external-model		
			model-version		
UpdateDetectorVersionMetadata	Gewährt die Berechtigung zum Aktualisieren der Beschreibung der Detektorversion. Sie können die Metadaten für jede Detektorversion (DRAFT, ACTIVE oder INACTIVE) aktualisieren.	Write	detector-version*		
UpdateDetectorVersionStatus	Gewährt die Berechtigung zum Aktualisieren des Status der Detektorversion. Mit UpdateDetectorVersionStatus können Sie die folgenden Aktionen oder Demos durchführen: DRAFT auf ACTIVE, ACTIVE auf INACTIVE und INACTIVE auf ACTIVE.	Schreiben	detector-version*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateEventLabel	Gewährt die Berechtigung zum Aktualisieren des Beschriftungswerts eines vorhandenen Ereignisdatensatzes	Schreiben	event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateList	Gewährt die Berechtigung zum Aktualisieren einer Liste	Schreiben	list*		
				aws:ResourceTag/${TagKey}	
UpdateModel	Gewährt die Berechtigung zum Aktualisieren einer Website. Mit dieser Aktion können Sie das Beschreibungsattribut aktualisieren.	Write	model*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateModelVersion	Gewährt die Berechtigung zum Aktualisieren einer Modellversion. Durch das Aktualisieren einer Modellversion wird eine vorhandene Modellversion mithilfe aktualisierter Trainingsdaten neu geschult, und es wird eine neue Nebenversion des Modells erstellt. Mit dieser Aktion können Sie den Speicherort des Trainingsdatensets und die Datenzugriffsrollenattribute aktualisieren. Diese Aktion erstellt und trainiert eine neue Nebenversion des Modells, zum Beispiel Version 1.01, 1.02, 1.03.	Write	model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateModelVersionStatus	Gewährt die Berechtigung zum Aktualisieren des Status einer Modellversion	Write	model-version*		
UpdateRuleMetadata	Gewährt die Berechtigung zum Aktualisieren der Metadaten einer Regel. Das Beschreibungsattribut kann aktualisiert werden.	Write	rule*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateRuleVersion	Gewährt die Berechtigung zum Aktualisieren einer Regelversion, die zu einer neuen Regelversion führt. Aktualisiert eine Regelversion, was zu einer neuen Regelversion (Version 1,2,3...) führt.	Write	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateVariable	Gewährt die Berechtigung zum Aktualisieren einer Variablen	Write	variable*		

Vom Amazon Fraud Detector definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
batch-prediction	`arn:${Partition}:frauddetector:${Region}:${Account}:batch-prediction/${ResourcePath}`	aws:ResourceTag/${TagKey}
detector	`arn:${Partition}:frauddetector:${Region}:${Account}:detector/${ResourcePath}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
detector-version	arn:${Partition}:frauddetector:${Region}:${Account}:detector-version/${ResourcePath}	aws:ResourceTag/${TagKey}
entity-type	arn:${Partition}:frauddetector:${Region}:${Account}:entity-type/${ResourcePath}	aws:ResourceTag/${TagKey}
external-model	arn:${Partition}:frauddetector:${Region}:${Account}:external-model/${ResourcePath}	aws:ResourceTag/${TagKey}
event-type	arn:${Partition}:frauddetector:${Region}:${Account}:event-type/${ResourcePath}	aws:ResourceTag/${TagKey}
label	arn:${Partition}:frauddetector:${Region}:${Account}:label/${ResourcePath}	aws:ResourceTag/${TagKey}
model	arn:${Partition}:frauddetector:${Region}:${Account}:model/${ResourcePath}	aws:ResourceTag/${TagKey}
model-version	arn:${Partition}:frauddetector:${Region}:${Account}:model-version/${ResourcePath}	aws:ResourceTag/${TagKey}
outcome	arn:${Partition}:frauddetector:${Region}:${Account}:outcome/${ResourcePath}	aws:ResourceTag/${TagKey}
rule	arn:${Partition}:frauddetector:${Region}:${Account}:rule/${ResourcePath}	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
variable	`arn:${Partition}:frauddetector:${Region}:${Account}:variable/${ResourcePath}`	aws:ResourceTag/${TagKey}
batch-import	`arn:${Partition}:frauddetector:${Region}:${Account}:batch-import/${ResourcePath}`	aws:ResourceTag/${TagKey}
list	`arn:${Partition}:frauddetector:${Region}:${Account}:list/${ResourcePath}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Fraud Detector

Amazon Fraud Detector definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf den Markierungen, die in der Anforderung übergeben werden.	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf den Markierungen, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert Aktionen basierend auf den Tag-Schlüsseln, die in der Anforderung übergeben werden.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Free Tier

AWS Free Tier (Servicepräfix: `freetier`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Free Tier definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetFreeTierAlertPreference [nur Berechtigung]	Gewährt die Berechtigung zum Erhalt der Präferenz für kostenlose Benachrichtigungen (E-Mail-Adresse)	Lesen			
GetFreeTierUsage	Gewährt die Berechtigung zum Abrufen der Nutzungslimits des kostenlosen Kontingents und des MTD-Nutzungsstatus	Lesen			
PutFreeTierAlertPr	Gewährt die Berechtigung zum Einrichten der Benachrichtigungspräferenz für des	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
eference [nur Berechtigung]	kostenlosen Kontingents (E-Mail-Adresse)				

Von AWS Free Tier definierte Ressourcentypen

AWS Free Tier unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf AWS Free Tier zuzulassen, geben Sie in Ihrer Richtlinie `"Resource": "*"` an.

Bedingungsschlüssel für AWS Free Tier

Free Tier besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon FreeRTOS

Amazon FreeRTOS (Servicepräfix: `freertos`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon FreeRTOS definierte Aktionen
- Von Amazon FreeRTOS definierte Ressourcentypen
- Bedingungsschlüssel für Amazon FreeRTOS

Von Amazon FreeRTOS definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSoftwareConfiguration	Gewährt die Berechtigung zum Erstellen einer Softwarekonfiguration	Schreiben	configuration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscription	Gewährt die Berechtigung zum Erstellen eines Abonnements für den erweiterten FreeRTOS-Wartungsplan (EMP)	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSoftwareConfiguration	Gewährt die Berechtigung zum Löschen der Softwarekonfiguration	Schreiben	configuration*		
DescribeHardwarePlatform	Gewährt die Berechtigung zum Beschreiben der Hardware-Plattform	Lesen			
DescribeSoftwareConfiguration	Gewährt die Berechtigung zum Beschreiben der Softwarekonfiguration	Lesen	configuration*		
DescribeSubscription	Gewährt die Berechtigung zum Beschreiben des Abonnements für den erweitert	Lesen	subscription*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	en FreeRTOS-Wartungsplan (EMP)				
GetEmpPatchUrl	Gewährt die Berechtigung zum Abrufen der URL für Software-Patch-Release, Patch-Diff und Versionshinweise im Rahmen des erweiterten FreeRTOS-Wartungsplans (EMP)	Lesen			
GetSoftwareURL	Gewährt die Berechtigung zum Abrufen der URL für den Download der Amazon-FreeRTOS-Software	Lesen			
GetSoftwareURLForConfiguration	Gewährt die Berechtigung zum Abrufen der URL für den Download der Amazon-FreeRTOS-Software basierend auf der Konfiguration	Lesen			
GetSubscriptionBillingAmount	Gewährt die Berechtigung zum Abrufen des Abonnement-Rechnungsbetrags für den erweiterten FreeRTOS-Wartungsplan (EMP)	Lesen			
ListFreeRTOSVersions	Erteilt die Erlaubnis, Versionen von AmazonFree RTOS aufzulisten	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListHardwarePlatforms	Gewährt die Berechtigung zum Auflisten der Hardwareplattformen	Auflisten			
ListHardwareVendors	Gewährt die Berechtigung zum Auflisten der Hardwareanbieter	Auflisten			
ListSoftwareConfigurations	Gewährt die Berechtigung zum Auflisten der Softwarekonfigurationen	Auflisten			
ListSoftwarePatches	Gewährt die Berechtigung zum Auflisten von Software-Patches des Abonnements für den erweiterten FreeRTOS-Wartungsplan (EMP)	Auflisten			
ListSubscriptionEmails	Gewährt die Berechtigung zum Auflisten der Abonnement-E-Mails für den erweiterten FreeRTOS-Wartungsplan (EMP)	Auflisten			
ListSubscriptions	Gewährt die Berechtigung zum Auflisten der Abonnements für den erweiterten FreeRTOS-Wartungsplan (EMP)	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateEmailRecipients	Gewährt die Berechtigung zum Aktualisieren der Liste der Abonnement-E-Mail-Adressen für den erweiterten FreeRTOS-Wartungsplan (EMP)	Schreiben			
UpdateSoftwareConfiguration	Gewährt die Berechtigung zum Aktualisieren der Softwarekonfiguration	Schreiben	configuration*		
VerifyEmail	Gewährt die Berechtigung zum Verifizieren der E-Mail für den erweiterten FreeRTOS-Wartungsplan (EMP)	Schreiben			

Von Amazon FreeRTOS definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
configuration	`arn:${Partition}:freertos:${Region}:${Account}:configuration/${ConfigurationName}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
subscription	`arn:${Partition}:freertos:${Region}:${Account}:subscription/${SubscriptionID}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon FreeRTOS

Amazon FreeRTOS definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Tag-Schlüssel, der in der Anfrage des Benutzers an Amazon FreeRTOS enthalten ist	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach einer Tag-Schlüsselkomponente, die an eine Amazon FreeRTOS FreeRTOS-Ressource angehängt ist	String
aws:TagKeys	Filtert Zugriff nach der Liste aller Tag-Schlüsselnamen, die der Ressource in der Anforderung zugeordnet sind	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon FSx

Amazon FSx (Servicepräfix: `fsx`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon FSx definierte Aktionen
- Von Amazon FSx definierte Ressourcentypen
- Bedingungsschlüssel für Amazon FSx

Von Amazon FSx definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateFileGateway [nur Berechtigung]	Gewährt die Berechtigung zum Verknüpfen einer File Gateway-Instance mit einem Amazon FSx for Windows File Server-Dateisystem	Write	file-system*		
AssociateFileSystemAliases	Gewährt die Berechtigung zum Zuordnen von DNS-Aliassen zu einem Amazon FSx for Windows File Server-Dateisystem	Schreiben	file-system*		
BypassSnaplockEnterpriseRetention [nur Berechtigung]	Gewährt die Berechtigung zum Löschen eines FSx for ONTAP SnapLock Enterprise-Volumes, das WORM-Dateien (Write Once, Read Many) mit aktiven Aufbewahrungszeiträumen enthält	Berechtigungsverwaltung	volume*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelDataRepositoryTask	Gewährt die Berechtigung zum Abbrechen einer Daten-Repository-Aufgabe	Write	task*		
CopyBackup	Gewährt die Berechtigung zum Kopieren eines Backups	Schreiben	backup*		fsx:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CopySnapshotAndUpdateVolume	Gewährt die Berechtigung, ein vorhandenes Volume mithilfe eines Snapshots aus einem anderen Amazon FSx for OpenZFS-Dateisystem zu aktualisieren	Schreiben	snapshot*		
			volume*		
CreateBackup	Gewährt die Berechtigung zum Erstellen eines neuen Backups eines Amazon FSx-Dateisystems	Schreiben	backup*		fsx:TagResource
			file-system		
			volume		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataRepositoryAssociation	Gewährt die Berechtigung zum Erstellen einer neuen Daten-Repository-Zuordnung für ein Amazon-FSx-for-Lustre-Dateisystem	Schreiben	association*		fsx:TagResource
			file-system*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataRepositoryTask	Gewährt die Berechtigung zum Erstellen einer neuen Daten-Repository-Aufgabe für ein Amazon FSx for Lustre-Dateisystem	Schreiben	file-system*		fsx:TagResource
			task*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateFileCache	Erteilt die Berechtigung zum Erstellen eines neuen, leeren Amazon-Datei-Caches	Schreiben	file-cache*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:GetSecurityGroupsForVpc fsx:CreateDataRepositoryAssociation fsx:TagResource logs:CreateLogGroup logs:CreateLogStream logs:PutLogEvents

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					s3:ListBucket
			association	fsx:NfsDataRepositoryEncryptionInTransitEnabled fsx:NfsDataRepositoryAuthenticationEnabled	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFileSystem	Gewährt die Berechtigung zum Erstellen eines neuen, leeren Amazon FSx-Dateisystems	Schreiben	file-system*		ec2:GetSecurityGroupsForVpc fsx:TagResource

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFileSystemFromBackup	Gewährt die Berechtigung zum Erstellen eines neuen Amazon FSx-Dateisystems aus einem vorhandenen Backup	Schreiben	backup*		ec2:GetSecurityGroupsForVpc fsx:TagResource
			file-system*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshot	Gewährt die Berechtigung zum Erstellen eines neuen Snapshots auf einem Volumen	Schreiben	snapshot*		fsx:TagResource
			volume*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStorageVirtualMachine	Gewährt die Berechtigung zum Erstellen einer neuen virtuellen Speichermaschine in einem Amazon FSx for Ontap Dateisystem	Schreiben	file-system*		fsx:TagResource
			storage-virtual-machine*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVolume	Gewährt die Berechtigung zum Erstellen eines neuen Volumes	Schreiben	volume*		fsx:TagResource
			snapshot		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId fsx:ParentVolumeId	
CreateVolumeFromBackup	Gewährt die Berechtigung zum Erstellen eines neuen Volumes von einem Backup	Schreiben	backup*		fsx:TagResource
			storage-virtual-machine*		
			volume*		
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteBackup	Gewährt die Berechtigung zum Löschen eines Backups, wobei der Inhalt gelöscht wird. Nach dem Löschen ist das Backup nicht länger vorhanden und auch dessen Daten sind nicht mehr verfügbar	Schreiben	backup*		
DeleteDataRepositoryAssociation	Gewährt die Berechtigung zum Löschen einer Daten-Repository-Zuordnung	Schreiben	association*		
DeleteFileCache	Erteilt die Berechtigung zum Löschen eines Datei-Caches, wobei der Inhalt gelöscht wird	Schreiben	file-cache*		fsx:DeleteDataRepositoryAssociation
			association		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteFileSystem	Gewährt die Berechtigung zum Löschen eines Dateisystems, wobei der Inhalt sowie alle vorhandenen automatischen Sicherungen des Dateisystems gelöscht werden	Schreiben	file-system*		fsx:CreateBackup fsx:TagResource
			backup		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteResourcePolicy [nur Berechtigung]	Erforderlich für die Verwaltung der kontoübergreifenden Freigabe von FSx-Volumes über AWS Resource Access Manager (RAM). PutResourcePolicy Außerdem GetResourcePolicy sind sie erforderlich.	Berechtigungsverwaltung	volume*		
DeleteSnapshot	Gewährt die Berechtigung zum Löschen eines Snapshots eines Volumes	Schreiben	snapshot*		
DeleteStorageVirtualMachine	Gewährt die Berechtigung zum Löschen einer virtuellen Speichermaschine, wobei der Inhalt gelöscht wird	Schreiben	storage-virtual-machine*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteVolume	Gewährt die Berechtigung zum Löschen eines Volumes, wobei der Inhalt sowie alle vorhandenen automatischen Backups des Volumes gelöscht werden	Schreiben	volume*		fsx:TagResource
			backup		
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId fsx:ParentVolumeId	
DescribeAssociatedFileGateways [nur Berechtigung]	Gewährt die Berechtigung zur Beschreibung der File Gateway-Instances, die mit einem Amazon FSx for Windows File Server-Dateisystem verknüpft sind	Read	file-system*		
DescribeBackups	Gewährt die Berechtigung zum Zurückgeben von Beschreibungen aller Backups, die zu Ihrem AWS-Konto in der AWS-Region des von Ihnen aufgerufenen Endpunkts gehören	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDataRepositoryAssociations	Gewährt die Berechtigung zum Zurückgeben von Beschreibungen aller Daten-Repository-Zuordnungen, die zu Ihrem AWS-Konto in der AWS-Region des von Ihnen aufgerufenen Endpunkts gehören	Lesen			
DescribeDataRepositoryTasks	Gewährt die Berechtigung zum Zurückgeben von Beschreibungen aller Daten-Repository-Aufgaben, die zu Ihrem AWS-Konto in der AWS-Region des von Ihnen aufgerufenen Endpunkts gehören	Lesen			
DescribeFileCaches	Erteilt die Berechtigung zum Zurückgeben der Beschreibungen aller Datei-Caches, die zu Ihrem AWS-Konto in der AWS-Region des von Ihnen aufgerufenen Endpunkts gehören	Lesen			
DescribeFileSystemAliases	Gewährt die Berechtigung zum Zurückgeben der Beschreibung aller DNS-Aliase im Besitz Ihres Amazon FSx for Windows File Server-Dateisystems	Read	file-system*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeFileSystems	Gewährt die Berechtigung zum Zurückgeben der Beschreibungen aller Dateisysteme, die zu Ihrem AWS-Konto in der AWS-Region des von Ihnen aufgerufenen Endpunkts gehören	Lesen			
DescribeSharedVpcConfiguration	Gewährt die Berechtigung, die Beschreibungen zurückzugeben, ob FSx-Routingtabellenaktualisierungen von Teilnehmerkonten in Ihrem Konto erlaubt sind	Lesen			
DescribeSnapshots	Gewährt die Berechtigung zum Zurückgeben von Beschreibungen aller Sicherungen, die zu Ihrem AWS-Konto in der AWS-Region des von Ihnen aufgerufenen Endpunkts gehören	Lesen			
DescribeStorageVirtualMachines	Gewährt die Berechtigung zum Zurückgeben von Beschreibungen aller virtuellen Speichermaschinen, die zu Ihrem AWS-Konto in der AWS-Region des von Ihnen aufgerufenen Endpunkts gehören	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeVolumes	Gewährt die Berechtigung zum Zurückgeben von Beschreibungen aller Volumes, die zu Ihrem AWS-Konto in der AWS-Region des von Ihnen aufgerufenen Endpunkts gehören	Lesen			
DisassociateFileGateway [nur Berechtigung]	Gewährt die Berechtigung zum Trennen einer File Gateway-Instance von einem Amazon FSx for Windows File Server-Dateisystem	Write	file-system*		
DisassociateFileSystemAliases	Gewährt die Berechtigung zum Trennen der Mapping von Dateisystem-Aliassen zu einem Amazon FSx for Windows File Server-Dateisystem	Schreiben	file-system*		
GetResourcePolicy [nur Berechtigung]	Erforderlich für die Verwaltung der kontoübergreifenden Freigabe von FSx-Volumes über AWS Resource Access Manager (RAM). PutResourcePolicy Außerdem DeleteResourcePolicy sind sie erforderlich.	Berechtigungsverwaltung	volume*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Amazon FSx-Ressource	Lesen	association		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			backup		
			file-cache		
			file-system		
			snapshot		
			storage-virtual-machine		
			task		
			volume		
ManageBackupPrincipalAssociations [nur Berechtigung]	Gewährt die Berechtigung zur Verwaltung von Backup-Principal-Mappings über AWS Backup	Berechtigungsverwaltung	backup*		
PutResourcePolicy [nur Berechtigung]	Erforderlich für die Verwaltung der kontoübergreifenden Freigabe von FSx-Volumes über AWS Resource Access Manager (RAM). DeleteResourcePolicy Außerdem GetResourcePolicy sind sie erforderlich.	Berechtigungsverwaltung	volume*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ReleaseFileSystemNfsV3Locks	Erteilt die Berechtigung, NFS V3-Sperren des Dateisystems freizugeben	Schreiben	file-system*		
RestoreVolumeFromSnapshot	Gewährt die Berechtigung zum Wiederherstellen des Volume-Zustands aus einem Snapshot	Schreiben	snapshot*		
			volume*		
StartMisconfiguredStateRecovery	Gewährt die Berechtigung zum Starten der falsch konfigurierten Statuswiederherstellung	Schreiben	file-system*		
TagResource	Gewährt die Berechtigung zum Markieren einer Amazon FSx-Ressource	Markieren	association		
			backup		
			file-cache		
			file-system		
			snapshot		
			storage-virtual-machine		
			task		
			volume		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen eines Tags aus einer Amazon FSx-Ressource	Tagging	association		
			backup		
			file-cache		
			file-system		
			snapshot		
			storage-virtual-machine		
			task		
			volume		
				aws:TagKeys	
UpdateDataRepositoryAssociation	Gewährt die Berechtigung zum Aktualisieren der Konfiguration einer Daten-Repository-Zuordnung	Schreiben	association*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateFileCache	Erteilt die Berechtigung zum Aktualisieren der Datei-Cache-Konfiguration	Schreiben	file-cache*		
UpdateFileSystem	Gewährt die Berechtigung zum Aktualisieren der Dateisystemkonfiguration	Schreiben	file-system*		
UpdateSharedVpcConfiguration	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren der Aktualisierungen der FSx-Routingtabelle von Teilnehmerkonten in Ihrem Konto	Schreiben			
UpdateSnapshot	Gewährt die Berechtigung zum Aktualisieren einer Snapshot-Konfiguration	Schreiben	snapshot*		
UpdateStorageVirtualMachine	Gewährt die Berechtigung zum Aktualisieren einer virtuellen Speichermaschine	Schreiben	storage-virtual-machine*		
UpdateVolume	Gewährt die Berechtigung zum Aktualisieren einer Volume-Konfiguration.	Schreiben	volume*		
				fsx:StorageVirtualMachineId fsx:ParentVolumeId	

Von Amazon FSx definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

> **Note**
>
> Amazon FSx for Windows File Server und Amazon FSx for Lustre teilen einige der gleichen Ressourcentypen mit jeweils demselben ARN-Format.

Ressourcentypen	ARN	Bedingungsschlüssel
file-system	`arn:${Partition}:fsx:${Region}:${Account}:file-system/${FileSystemId}`	aws:ResourceTag/${TagKey}
file-cache	`arn:${Partition}:fsx:${Region}:${Account}:file-cache/${FileCacheId}`	aws:ResourceTag/${TagKey}
backup	`arn:${Partition}:fsx:${Region}:${Account}:backup/${BackupId}`	aws:ResourceTag/${TagKey}
storage-virtual-machine	`arn:${Partition}:fsx:${Region}:${Account}:storage-virtual-machine/${FileSystemId}/${StorageVirtualMachineId}`	aws:ResourceTag/${TagKey}
task	`arn:${Partition}:fsx:${Region}:${Account}:task/${TaskId}`	aws:ResourceTag/${TagKey}
association	`arn:${Partition}:fsx:${Region}:${Account}:association/${FileSystemIdOrFileCacheId}/${DataRepositoryAssociationId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
volume	`arn:${Partition}:fsx:${Region}:${Account}:volume/${FileSystemId}/${VolumeId}`	aws:ResourceTag/${TagKey}
snapshot	`arn:${Partition}:fsx:${Region}:${Account}:snapshot/${VolumeId}/${SnapshotId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon FSx

Amazon FSx definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString
fsx:IsBackupCopyDestination	Filtert den Zugriff danach, ob das Backup ein Ziel-Backup für eine CopyBackup Operation ist	Bool

Bedingungsschlüssel	Beschreibung	Typ
fsx:IsBackupCopySource	Filtert den Zugriff danach, ob das Backup ein Quell-Backup für eine - CopyBackup Operation ist	Bool
fsx:NfsDataRepositoryAuthenticationEnabled	Filtert den Zugriff nach NFS-Datenrepositorys, die Authentifizierung unterstützen	Bool
fsx:NfsDataRepositoryEncryptionInTransitEnabled	Filtert den Zugriff nach NFS-Datenrepositories, die unterstützen encryption-in-transit	Bool
fsx:ParentVolumeId	Filtert den Zugriff nach dem enthaltenden übergeordneten Volume für mutierende Volume-Operationen	String
fsx:StorageVirtualMachineId	Filtert den Zugriff durch die enthaltende virtuelle Speichermaschine für ein Volume zum Mutieren von Volume-Vorgängen	String

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon GameLift

Amazon GameLift (Service-Präfix:`gamelift`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon definierte Aktionen GameLift

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptMatch	Erteilt die Erlaubnis, zu registrieren, ob ein Spieler ein geplantes FlexMatch Spiel akzeptiert oder ablehnt	Schreiben			
ClaimGameServer	Gewährt die Berechtigung zum Suchen und Reservieren eines Spielservers für die Ausrichtung einer neuen Spielsitzung	Write	gameServerGroup*		
CreateAlias	Gewährt die Berechtigung, einen neuen Alias für eine Flotte zu definieren	Write		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreateBuild	Gewährt die Berechtigung zum Erstellen eines neuen Spiele-Builds mit Dateien, die in einem Amazon-S3-Bucket gespeichert sind	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource iam:PassRole s3:GetObject
CreateContainerGroupDefinition	Erteilt die Erlaubnis, eine neue Containergruppendefinition für eine Containerflotte zu erstellen	Schreiben		aws:RequestTag/${TagKey}	ecr:BatchGetImage

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	ecr:DescribeImages ecr:GetDownloadUrlForLayer gamelift:TagResource
CreateFleet	Gewährt die Berechtigung, eine neue Flotte von Datenverarbeitungsressourcen zum Ausführen der Spieleserver zu erstellen	Write		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeRegions gamelift:TagResource iam:PassRole
CreateFleetLocations	Gewährt die Berechtigung, zusätzliche Standorte für eine Flotte anzugeben	Write	fleet*		ec2:DescribeRegions

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateGameServerGroup	Gewährt die Berechtigung zum Erstellen einer neuen Spielserver-Gruppe, zum Einrichten einer entsprechenden Auto-Scaling-Gruppe und zum Starten von Instances, um für Spieleserver zu hosten	Write		aws:RequestTag/${TagKey} aws:TagKeys	autoscaling:CreateAutoScalingGroup autoscaling:DescribeAutoScalingGroups autoscaling:PutLifecycleHook autoscaling:PutScalingPolicy ec2:DescribeAvailabilityZones ec2:DescribeSubnets events:PutRule events:PutTargets

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					gamelift:TagResource iam:PassRole
CreateGameSession	Gewährt die Berechtigung zum Starten einer neuen Spielsitzung auf einer bestimmten Flotte	Write			
CreateGameSessionQueue	Gewährt die Berechtigung zum Einrichten einer neuen Warteschlange für die Verarbeitung von Anforderungen zur Platzierung von Spielsitzungen	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreateLocation	Gewährt die Berechtigung zum Definieren eines neuen Speicherorts für eine Flotte	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreateMatchmakingConfiguration	Erteilt die Erlaubnis, einen neuen FlexMatch Matchmaker zu erstellen	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateMatchmakingRuleSet	Erteilt die Erlaubnis, einen neuen Matchmaking-Regelsatz für zu erstellen FlexMatch	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreatePlayerSession	Gewährt die Berechtigung, einen verfügbaren Spielsitzungs-Slot für einen Spieler zu reservieren	Write			
CreatePlayerSessions	Gewährt die Berechtigung, verfügbare Spielsitzungs-Slots für mehrere Spieler zu reservieren	Write			
CreateScript	Gewährt die Berechtigung zum Erstellen eines neuen Realtime-Servers-Skripts	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource iam:PassRole s3:GetObject

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateVpcPeeringAuthorization	GameLift Erteilt die Berechtigung, eine Peering-Verbindung zwischen einer GameLift Flotten-VPC und einer VPC auf einer anderen zu erstellen oder zu löschen AWS-Konto	Schreiben			ec2:AcceptVpcPeeringConnection ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateRoute ec2:DeleteRoute ec2:DescribeRouteTables ec2:DescribeSecurityGroups ec2:RevokeSecurityGroupEgress

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ec2:RevokeSecurityGroupIngress
CreateVpcPeeringConnection	Erteilt die Erlaubnis, eine Peering-Verbindung zwischen Ihrer GameLift Flotten-VPC und einer VPC auf einem anderen Konto herzustellen	Schreiben			
DeleteAlias	Gewährt die Berechtigung zum Löschen eines Alias	Write	alias*		
DeleteBuild	Gewährt die Berechtigung zum Löschen eines Spiele-Builds	Schreiben	build*		
DeleteContainerGroupDefinition	Erteilt die Berechtigung zum Löschen einer Container-Gruppendefinition, die nicht in einer Flotte verwendet wird	Schreiben	containerGroupDefinition*		
DeleteFleet	Gewährt die Berechtigung zum Löschen einer leeren Flotte	Write	fleet*		
DeleteFleetLocations	Gewährt die Berechtigung zum Löschen von Standorten für eine Flotte	Write	fleet*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteGameServerGroup	Gewährt die Berechtigung, eine Spieleserver-Gruppe dauerhaft zu löschen und die FleetIQ-Aktivität für die entsprechende Auto-Scaling-Gruppe zu beenden	Write	gameServerGroup*		autoscaling:DeleteAutoScalingGroup autoscaling:DescribeAutoScalingGroups autoscaling:ExitStandby autoscaling:ResumeProcesses autoscaling:SetInstanceProtection autoscaling:UpdateAutoScalingGroup
DeleteGameSessionQueue	Gewährt die Berechtigung zum Löschen einer vorhandenen Spielsitzungswarteschlange	Schreiben	gameSessionQueue*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteLocation	Gewährt die Berechtigung zum Löschen eines Speicherorts	Schreiben	location*		
DeleteMatchmakingConfiguration	Erteilt die Erlaubnis, einen vorhandenen FlexMatch Matchmaker zu löschen	Schreiben	matchmakingConfiguration*		
DeleteMatchmakingRuleSet	Erteilt die Erlaubnis, einen vorhandenen FlexMatch Matchmaking-Regelsatz zu löschen	Schreiben	matchmakingRuleSet*		
DeleteScalingPolicy	Gewährt die Berechtigung zum Löschen einer Reihe von Auto-Scaling-Regeln	Write	fleet*		
DeleteScript	Gewährt die Berechtigung zum Löschen eines Realtime-Servers-Skripts	Write	script*		
DeleteVpcPeeringAuthorization	Gewährt die Berechtigung, eine VPC-Peering-Autorisierung zu stornieren	Write			
DeleteVpcPeeringConnection	Gewährt die Berechtigung zum Entfernen einer Peering-Verbindung zwischen VPCs	Schreiben			
DeregisterCompute	Gewährt die Berechtigung zum Aufheben der Registrierung eines Rechners für eine Flotte	Schreiben	fleet*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeregisterGameServer	Gewährt die Berechtigung zum Entfernen eines Spieleservers aus einer Spieleserver-Gruppe	Write	gameServerGroup*		
DescribeAlias	Gewährt die Berechtigung zum Abrufen von Eigenschaften für einen Alias	Read	alias*		
DescribeBuild	Gewährt die Berechtigung zum Abrufen von Eigenschaften für einen Spiele-Build	Lesen	build*		
DescribeCompute	Gewährt die Berechtigung zum Abrufen allgemeiner Eigenschaften des Computers wie ARN, Flottendetails, SDK-Endpunkte und Speicherort	Lesen	fleet*		
DescribeContainerGroupDefinition	Erteilt die Berechtigung zum Abrufen allgemeiner Eigenschaften, einschließlich des Status, für eine Container-Gruppendefinition	Lesen	containerGroupDefinition*		
DescribeEC2InstanceLimits	Gewährt die Berechtigung zum Abrufen der maximal zulässigen und aktuellen Nutzung für EC2-Instance-Typen	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeFleetAttributes	Gewährt die Berechtigung zum Abrufen von allgemeinen Eigenschaften, einschließlich des Status, für Flotten	Read			
DescribeFleetCapacity	Gewährt die Berechtigung zum Abrufen der aktuellen Kapazitätseinstellung für Flotten	Read			
DescribeFleetEvents	Gewährt die Berechtigung zum Abrufen von Einträgen aus dem Ereignisprotokoll einer Flotte	Read	fleet*		
DescribeFleetLocationAttributes	Gewährt die Berechtigung zum Abrufen von allgemeinen Eigenschaften, einschließlich des Status, für die Standorte einer Flotte	Read	fleet*		
DescribeFleetLocationCapacity	Gewährt die Berechtigung zum Abrufen der aktuellen Kapazitätseinstellung für den Standort einer Flotte	Read	fleet*		
DescribeFleetLocationUtilization	Gewährt die Berechtigung zum Abrufen von Nutzungsstatistiken für den Standort der Flotte	Read	fleet*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeFleetPortSettings	Gewährt die Berechtigung zum Abrufen der Berechtigungen für eingehende Verbindungen für eine Flotte	Read	fleet*		
DescribeFleetUtilization	Gewährt die Berechtigung zum Abrufen von Nutzungsstatistiken für Flotten	Read			
DescribeGameServer	Gewährt die Berechtigung zum Abrufen von Eigenschaften für einen Spieleserver	Read	gameServerGroup*		
DescribeGameServerGroup	Gewährt die Berechtigung zum Abrufen von Eigenschaften für eine Spieleserver-Gruppe	Read	gameServerGroup*		
DescribeGameServerInstances	Gewährt die Berechtigung zum Abrufen des Status von EC2-Instances in einer Spieleserver-Gruppe	Read	gameServerGroup*		
DescribeGameSessionDetails	Gewährt die Berechtigung zum Abrufen von Eigenschaften für Spielsitzungen in einer Flotte, einschließlich der Schutzrichtlinie	Read			
DescribeGameSessionPlacement	Gewährt die Berechtigung zum Abrufen von Details einer Platzierungsanforderung für Spielsitzungen	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeGameSessionQueues	Gewährt die Berechtigung zum Abrufen von Eigenschaften für Spielsitzungswarteschlangen	Read			
DescribeGameSessions	Gewährt die Berechtigung zum Abrufen von Eigenschaften für Spielsitzungen in einer Flotte	Read			
DescribeInstances	Gewährt die Berechtigung zum Abrufen von Informationen über Instances in einer Flotte	Read	fleet*		
DescribeMatchmaking	Gewährt die Berechtigung zum Abrufen von Details zu Matchmaking-Tickets	Lesen			
DescribeMatchmakingConfigurations	Erteilt FlexMatch Matchmakers die Erlaubnis, Eigenschaften abzurufen	Lesen			
DescribeMatchmakingRuleSets	Erteilt die Erlaubnis zum Abrufen von Eigenschaften für FlexMatch Matchmaking-Regelsätze	Lesen			
DescribePlayerSessions	Gewährt die Berechtigung zum Abrufen von Eigenschaften für Spielersitzungen in einer Spielsitzung	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeRuntimeConfiguration	Gewährt die Berechtigung zum Abrufen der aktuellen Laufzeitkonfiguration für eine Flotte	Read	fleet*		
DescribeScalingPolicies	Gewährt die Berechtigung zum Abrufen aller Skalierungsrichtlinien, die auf eine Flotte angewendet werden	Read	fleet*		
DescribeScript	Gewährt die Berechtigung zum Abrufen von Eigenschaften für ein Realtime-Servers-Skript	Read	script*		
DescribeVpcPeeringAuthorizations	Gewährt die Berechtigung zum Abrufen gültiger VPC-Peering-Autorisierungen	Read			
DescribeVpcPeeringConnections	Gewährt die Berechtigung zum Abrufen von Details zu aktiven oder ausstehenden VPC-Peering-Verbindungen	Lesen			
GetComputeAccess	Gewährt die Berechtigung zum Abrufen der Zugriffsrichtlinie eines Computers	Lesen	fleet*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetComputeAuthToken	Gewährt die Berechtigung zum Abrufen eines Autorisierungstokens für einen Computer und eine Flotte, um es in Spielserverprozessen zu verwenden	Lesen	fleet*		
GetGameSessionLogUrl	Gewährt die Berechtigung zum Abrufen des Speicherorts von gespeicherten Protokollen für eine Spielsitzung	Read			
GetInstanceAccess	Gewährt die Berechtigung, Remote-Zugriff auf eine bestimmte Flotten-Instance anzufordern	Read	fleet*		
ListAliases	Gewährt die Berechtigung zum Abrufen aller Aliasse, die in der aktuellen Region definiert sind	List			
ListBuilds	Gewährt die Berechtigung zum Abrufen aller Spiele-Builds in der aktuellen Region	Auflisten			
ListCompute	Gewährt die Berechtigung zum Abrufen aller Datenverarbeitungsressourcen in der aktuellen Region	Auflisten	fleet*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListContainerGroupDefinitions	Erteilt die Berechtigung zum Abrufen einer Liste mit Namen für alle Containergruppendefinitionen in der aktuellen Region	Auflisten			
ListFleets	Gewährt die Berechtigung zum Abrufen einer Liste von Flotten-IDs für alle Flotten in der aktuellen Region	List			
ListGameServerGroups	Gewährt die Berechtigung zum Abrufen aller Spieleserver-Gruppen, die in der aktuellen Region definiert sind	List			
ListGameServers	Gewährt die Berechtigung zum Abrufen aller Spieleserver, die derzeit in einer Spieleserver-Gruppe ausgeführt werden	Auflisten	gameServerGroup*		
ListLocations	Gewährt die Berechtigung zum Abrufen aller Speicherorte in diesem Konto	Auflisten			
ListScripts	Gewährt die Berechtigung zum Abrufen von Eigenschaften für alle Realtime-Servers-Skripts in der aktuellen Region	Auflisten			
ListTagsForResource		Lesen	alias		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Erteilt die Berechtigung zum Abrufen von Tags für GameLift Ressourcen		build		
			containerGroupDefinition		
			fleet		
			gameServerGroup		
			gameSessionQueue		
			location		
			matchmakingConfiguration		
			matchmakingRuleSet		
			script		
PutScalingPolicy	Gewährt die Berechtigung zum Erstellen oder Aktualisieren einer Auto-Scaling-Richtlinie für die Flotte	Schreiben	fleet*		
RegisterCompute	Gewährt die Berechtigung zum Registrieren eines Rechners für eine Flotte	Schreiben	fleet*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RegisterGameServer	Erteilt die Erlaubnis, GameLift FleetIQ zu benachrichtigen, wenn ein neuer Spieleserver bereit ist, das Gameplay zu hosten	Schreiben	gameServerGroup*		
RequestUploadCredentials	Gewährt die Berechtigung zum Abrufen neuer Upload-Anmeldeinformationen, die beim Hochladen eines neuen Spiele-Builds verwendet werden sollen	Read	build*		
ResolveAlias	Gewährt die Berechtigung, die mit einem Alias verbundene Flotten-ID abzurufen	Read	alias*		
ResumeGameServerGroup	Gewährt die Berechtigung zum Wiederherstellen gesperrter FleetIQ-Aktivitäten für eine Spieleserver-Gruppe	Write	gameServerGroup*		
SearchGameSessions	Gewährt die Berechtigung zum Abrufen von Spielsitzungen, die einer Reihe von Suchkriterien entsprechen	Lesen			
StartFleetActions	Erteilt die Erlaubnis, die Auto-Scaling-Aktivität für eine Flotte wieder aufzunehmen, nachdem sie mit StopFleet Actions () angehalten wurde	Schreiben	fleet*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartGameSessionPlacement	Gewährt die Berechtigung zum Senden einer Anfrage zur Platzierung einer Spielesitzung an eine Spielesitzungs-Warteschlange	Schreiben	gameSessionQueue*		
StartMatchBackfill	Erlaubt die Erlaubnis, FlexMatch Spielersuche anzufordern, um verfügbare Spielerplätze in einer bestehenden Spielsitzung zu besetzen	Schreiben			
StartMatchmaking	Erteilt die Erlaubnis, FlexMatch Spielersuche für einen oder mehrere Spieler anzufordern und die Platzierung einer Spielsitzung einzuleiten	Schreiben			
StopFleetActions	Gewährt die Berechtigung, Auto-Scaling-Aktivitäten in einer Flotte auszusetzen	Write	fleet*		
StopGameSessionPlacement	Gewährt die Berechtigung zum Abbrechen einer laufenden Platzierungsanfrage für Spielesitzungen	Write			
StopMatchmaking	Gewährt die Berechtigung, eine laufende Matchmaking- oder Match-Backfill-Anfrage abzubrechen	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SuspendGameServerGroup	Gewährt die Berechtigung, die FleetIQ-Aktivitäten für eine Spieleserver-Gruppe vorübergehend zu beenden	Schreiben	gameServerGroup*		
TagResource	Erteilt die Erlaubnis, Ressourcen zu taggen GameLift	Tagging	alias		
			build		
			containerGroupDefinition		
			fleet		
			gameServerGroup		
			gameSessionQueue		
			location		
			matchmakingConfiguration		
			matchmakingRuleSet		
			script		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Erteilt die Erlaubnis zum Aufheben der Markierung GameLift von Ressourcen	Tagging	alias		
			build		
			containerGroupDefinition		
			fleet		
			gameServerGroup		
			gameSessionQueue		
			location		
			matchmakingConfiguration		
			matchmakingRuleSet		
			script		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
UpdateAlias	Gewährt die Berechtigung, die Eigenschaften eines bestehenden Alias zu aktualisieren	Write	alias*		
UpdateBuild	Gewährt die Berechtigung, die Metadaten eines bestehenden Builds zu aktualisieren	Write	build*		
UpdateFleetAttributes	Gewährt die Berechtigung, die allgemeinen Eigenschaften einer bestehenden Flotte zu aktualisieren	Write	fleet*		
UpdateFleetCapacity	Gewährt die Berechtigung, die Kapazitätseinstellungen einer Flotte anzupassen	Write	fleet*		
UpdateFleetPortSettings	Gewährt die Berechtigung, die Porteinstellungen einer Flotte anzupassen	Write	fleet*		
UpdateGameServer	Gewährt die Berechtigung zum Ändern der Eigenschaften des Spieleservers, des Integritätsstatus oder des Nutzungsstatus	Write	gameServerGroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateGameServerGroup	Gewährt die Berechtigung zum Aktualisieren von Eigenschaften für Spieleserver-Gruppen, einschließlich zulässiger Instance-Typen	Write	gameServerGroup*		iam:PassRole
UpdateGameSession	Gewährt die Berechtigung, die Eigenschaften einer bestehenden Spielesitzung zu aktualisieren	Write			
UpdateGameSessionQueue	Gewährt die Berechtigung zum Aktualisieren von Eigenschaften einer vorhandenen Spielesitzungs-Warteschlange	Schreiben	gameSessionQueue*		
UpdateMatchmakingConfiguration	Erteilt die Erlaubnis, die Eigenschaften einer vorhandenen FlexMatch Matchmaking-Konfiguration zu aktualisieren	Schreiben	matchmakingConfiguration*		
UpdateRuntimeConfiguration	Gewährt die Berechtigung, zu aktualisieren, wie Serverprozesse für Instances in einer bestehenden Flotte konfiguriert werden	Write	fleet*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateScript	Gewährt die Berechtigung zum Aktualisieren der Metadaten und des Inhalts eines vorhandenen Realtime-Servers-Skripts	Schreiben	script*		iam:PassRole s3:GetObject
ValidateMatchmakingRuleSet	Erteilt die Erlaubnis, die Syntax eines FlexMatch Matchmaking-Regelsatzes zu überprüfen	Lesen			

Von Amazon definierte Ressourcentypen GameLift

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
alias	`arn:${Partition}:gamelift:${Region}::alias/${AliasId}`	aws:ResourceTag/${TagKey}
build	`arn:${Partition}:gamelift:${Region}:${Account}:build/${BuildId}`	aws:ResourceTag/${TagKey}
containerGroupDefinition	`arn:${Partition}:gamelift:${Region}:${Account}:containergroupdefinition/${Name}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
fleet	`arn:${Partition}:gamelift:${Region}:${Account}:fleet/${FleetId}`	aws:ResourceTag/${TagKey}
gameServerGroup	`arn:${Partition}:gamelift:${Region}:${Account}:gameservergroup/${GameServerGroupName}`	aws:ResourceTag/${TagKey}
gameSessionQueue	`arn:${Partition}:gamelift:${Region}:${Account}:gamesessionqueue/${GameSessionQueueName}`	aws:ResourceTag/${TagKey}
location	`arn:${Partition}:gamelift:${Region}:${Account}:location/${LocationId}`	aws:ResourceTag/${TagKey}
matchmakingConfiguration	`arn:${Partition}:gamelift:${Region}:${Account}:matchmakingconfiguration/${MatchmakingConfigurationName}`	aws:ResourceTag/${TagKey}
matchmakingRuleSet	`arn:${Partition}:gamelift:${Region}:${Account}:matchmakingruleset/${MatchmakingRuleSetName}`	aws:ResourceTag/${TagKey}
script	`arn:${Partition}:gamelift:${Region}:${Account}:script/${ScriptId}`	aws:ResourceTag/${TagKey}

Zustandsschlüssel für Amazon GameLift

Amazon GameLift definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Global Accelerator

AWS Global Accelerator (Servicepräfix: `globalaccelerator`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Global Accelerator definierte Aktionen
- Von AWS Global Accelerator definierte Ressourcentypen
- Bedingungsschlüssel für AWS Global Accelerator

Von AWS Global Accelerator definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddCustomRoutingEndpoints	Gewährt die Berechtigung, einer benutzerdefinierten Routing-Accelerator-Endpunktgruppe einen Virtual Private Cloud (VPC)-Subnetzendpunkt hinzuzufügen	Schreiben	endpointgroup*		
AddEndpoints	Gewährt die Berechtigung zum Hinzufügen eines Endpunkts zu einer Standard-Accelerator-Endpunktgruppe	Schreiben	endpointgroup*		globalaccelerator:UpdateEndpointGroup
AdvertiseByoipCidr	Gewährt die Berechtigung, einen IPv4-Adressbereich anzukündigen, der zur Verwendung mit Ihrem Accelerator mittels Bring Your Own IP (BYOIP) bereitgestellt wird	Schreiben			
AllowCustomRoutingTraffic	Gewährt die Berechtigung, das benutzerdefinierte Routing des Benutzerdatenverkehrs an einen privaten IP:PORT-Zielbereich in einem bestimmten VPC-Subnetz zuzulassen	Schreiben	endpointgroup*		
CreateAccelerator	Gewährt die Berechtigung zum Erstellen eines Standard-Accelerators	Schreiben		aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
CreateCrossAccountAttachment	Gewährt die Berechtigung zum Erstellen eines CrossAccountAttachment	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomRoutingAccelerator	Gewährt die Berechtigung zum Erstellen eines benutzerdefinierten Routing-Accelerators	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomRoutingEndpointGroup	Gewährt die Berechtigung zum Erstellen einer Endpunktgruppe für den angegebenen Listener eines benutzerdefinierten Routing-Accelerators	Schreiben	listener*		
CreateCustomRoutingListener	Gewährt die Berechtigung, einen Listener zu erstellen, um eingehende Verbindungen von Clients zu einem benutzerdefinierten Routing-Accelerator zu verarbeiten	Schreiben	accelerator*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateEndpointGroup	Gewährt die Berechtigung, einem Standard-Accelerator-Listener eine Endpunktgruppe hinzuzufügen	Schreiben	listener*		
CreateListener	Gewährt die Berechtigung, einem Standard-Accelerator einen Listener hinzuzufügen	Schreiben	accelerator*		
DeleteAccelerator	Gewährt die Berechtigung zum Löschen eines Standard-Accelerators	Schreiben	accelerator*		
DeleteCrossAccountAttachment	Gewährt die Berechtigung zum Löschen eines CrossAccountAttachment	Schreiben	attachment*		
DeleteCustomRoutingAccelerator	Gewährt die Berechtigung zum Löschen eines benutzerdefinierten Routing-Accelerators	Schreiben	accelerator*		
DeleteCustomRoutingEndpointGroup	Gewährt die Berechtigung zum Löschen einer Endpunktgruppe aus dem Listener eines benutzerdefinierten Routing-Accelerators	Schreiben	endpointgroup*		
DeleteCustomRoutingListener	Gewährt die Berechtigung zum Löschen eines Listeners für einen benutzerdefinierten Routing-Accelerator	Schreiben	listener*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteEndpointGroup	Gewährt die Berechtigung zum Löschen einer Endpunktgruppe, die mit einem Standard-Accelerator-Listener verknüpft ist	Schreiben	endpointgroup*		
DeleteListener	Gewährt die Berechtigung zum Löschen eines Listeners aus einem Standard-Accelerator	Schreiben	listener*		
DenyCustomRoutingTraffic	Gewährt die Berechtigung, das benutzerdefinierte Routing des Benutzerdatenverkehrs an einen privaten IP:PORT-Zielbereich in einem bestimmten VPC-Subnetz zu verweigern	Schreiben	endpointgroup*		
DeprovisionByoipCidr	Gewährt die Berechtigung, den angegebenen Adressbereich freizugeben, den Sie für die Verwendung mit Ihrem Accelerator mittels Bring Your Own IP (BYOIP) bereitgestellt haben	Schreiben			
DescribeAccelerator	Gewährt Berechtigungen zum Beschreiben eines Standard-Accelerators	Lesen	accelerator*		
DescribeAcceleratorAttributes	Gewährt die Berechtigung zum Beschreiben eines Standard-Accelerator-Attributs	Lesen	accelerator*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeCrossAccountAttachment	Gewährt die Berechtigung zum Beschreiben eines CrossAccountAttachment	Lesen	attachment*		
DescribeCustomRoutingAccelerator	Gewährt die Berechtigung zum Beschreiben eines benutzerdefinierten Routing-Accelerators	Lesen	accelerator*		
DescribeCustomRoutingAcceleratorAttributes	Gewährt die Berechtigung zum Beschreiben der Attribute eines benutzerdefinierten Routing-Accelerators	Lesen	accelerator*		
DescribeCustomRoutingEndpointGroup	Gewährt die Berechtigung zum Beschreiben einer Endpunktgruppe für einen benutzerdefinierten Routing-Accelerator	Lesen	endpointgroup*		
DescribeCustomRoutingListener	Gewährt die Berechtigung zum Beschreiben eines Listeners für einen benutzerdefinierten Routing-Accelerator	Lesen	listener*		
DescribeEndpointGroup	Gewährt die Berechtigung zum Beschreiben einer Standard-Accelerator-Endpunktgruppe	Lesen	endpointgroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeListener	Gewährt die Berechtigung zum Beschreiben eines Standard-Accelerator-Listeners	Lesen	listener*		
ListAccelerators	Gewährt die Berechtigung zum Auflisten aller Standard-Accelerators	Auflisten			
ListByoipCidrs	Gewährt die Berechtigung zum Auflisten der BYOIP-CIDRs	Auflisten			
ListCrossAccountAttachments	Gewährt die Berechtigung zum Auflisten aller CrossAccountAttachments	Auflisten			
ListCrossAccountResourceAccounts	Gewährt die Berechtigung zum Auflisten von Konten, bei denen CrossAccountAttachments den Anrufer als einen Prinzipal auflisten	Auflisten			
ListCrossAccountResources	Gewährt die Berechtigung zum Auflisten aller vom Anrufer verwendbaren CrossAccountAttachment	Auflisten			
ListCustomRoutingAccelerators	Gewährt die Berechtigung zum Auflisten der benutzerdefinierten Routing-Accelerators für ein AWS-Konto	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListCustomRoutingEndpointGroups	Gewährt die Berechtigung zum Auflisten der Endpunktgruppen, die mit dem Listener eines benutzerdefinierten Routing-Accelerators verknüpft sind	Auflisten	listener*		
ListCustomRoutingListeners	Gewährt die Berechtigung zum Auflisten der Listeners eines benutzerdefinierten Routing-Accelerators	Auflisten	accelerator*		
ListCustomRoutingPortMappings	Gewährt die Berechtigung zum Auflisten der Portmappings eines benutzerdefinierten Routing-Accelerators	Auflisten	accelerator*		
ListCustomRoutingPortMappingsByDestination	Gewährt die Berechtigung zum Auflisten der Portmappingen einer bestimmten Endpunkt-IP-Adresse (einer Zieladresse) in einem Subnetz	Auflisten			
ListEndpointGroups	Gewährt die Berechtigung zum Auflisten aller Endpunktgruppen, die mit einem Standard-Accelerator-Listener verknüpft sind	Auflisten	listener*		
ListListeners	Gewährt die Berechtigung zum Auflisten aller mit einem Standard-Accelerator verknüpften Listener	Auflisten	accelerator*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine GlobalAccelerator-Ressource	Lesen	accelerator		
			attachment		
ProvisionByoipCidr	Gewährt die Berechtigung, einen Adressbereich zur Verwendung mit Ihrem Accelerator mittels Bring Your Own IP (BYOIP) bereitzustellen	Schreiben			
RemoveCustomRoutingEndpoints	Gewährt die Berechtigung, Virtual Private Cloud (VPC)-Subnetzendpunkte aus einer benutzerdefinierten Routing-Accelerator-Endpunktgruppe zu entfernen	Schreiben	endpointgroup*		
RemoveEndpoints	Gewährt die Berechtigung zum Entfernen eines Endpunkts aus einer Standard-Accelerator-Endpunktgruppe	Schreiben	endpointgroup*		globalaccelerator:UpdateEndpointGroup
TagResource	Gewährt die Berechtigung, einer GlobalAccelerator-Ressource Tags hinzuzufügen	Markierung	accelerator		
			attachment		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung, Tags aus einer GlobalAccelerator-Ressource zu entfernen	Markierung	accelerator		
			attachment		
				aws:TagKeys	
UpdateAccelerator	Gewährt die Berechtigung zum Aktualisieren eines Standard-Accelerators	Schreiben	accelerator*		
UpdateAcceleratorAttributes	Gewährt die Berechtigung zum Aktualisieren von Standard-Accelerator-Attributen	Schreiben	accelerator*		
UpdateCrossAccountAttachment	Gewährt die Berechtigung zum Aktualisieren eines CrossAccountAttachment	Schreiben	attachment*		
UpdateCustomRoutingAccelerator	Gewährt die Berechtigung zum Aktualisieren eines benutzerdefinierten Routing-Accelerators	Schreiben	accelerator*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateCustomRoutingAcceleratorAttributes	Gewährt die Berechtigung zum Aktualisieren der Attribute eines benutzerdefinierten Routing-Accelerators	Schreiben	accelerator*		
UpdateCustomRoutingListener	Gewährt die Berechtigung zum Aktualisieren des Listeners eines benutzerdefinierten Routing-Accelerators	Schreiben	listener*		
UpdateEndpointGroup	Gewährt die Berechtigung zum Aktualisieren einer Endpunktgruppe in einem Standard-Accelerator-Listener	Schreiben	endpointgroup*		
UpdateListener	Gewährt die Berechtigung zum Aktualisieren eines Listeners in einem Standard-Accelerator	Schreiben	listener*		
WithdrawByoipCidr	Gewährt die Berechtigung, die Ankündigung einer BYOIP-IPv4-Adresse einzustellen	Schreiben			

Von AWS Global Accelerator definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
accelerator	`arn:${Partition}:globalaccelerator::${Account}:accelerator/${ResourceId}`	aws:ResourceTag/${TagKey}
listener	`arn:${Partition}:globalaccelerator::${Account}:accelerator/${ResourceId}/listener/${ListenerId}`	aws:ResourceTag/${TagKey}
endpointgroup	`arn:${Partition}:globalaccelerator::${Account}:accelerator/${ResourceId}/listener/${ListenerId}/endpoint-group/${EndpointGroupId}`	aws:ResourceTag/${TagKey}
attachment	`arn:${Partition}:globalaccelerator::${Account}:attachment/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Global Accelerator

AWS Global Accelerator definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Glue

AWS Glue (Dienstpräfix:`glue`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Glue definierte Aktionen
- Von AWS Glue definierte Ressourcentypen
- Bedingungsschlüssel für AWS Glue

Von AWS Glue definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchCreatePartition	Gewährt die Berechtigung zum Erstellen einer oder mehrerer Partitionen.	Write	catalog*		
			database*		
			table*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchDeleteConnection	Gewährt die Berechtigung zum Löschen einer oder mehrerer Verbindungen.	Write	catalog*		
			connection*		
BatchDeletePartition	Gewährt die Berechtigung zum Löschen einer oder mehrerer Partitionen.	Write	catalog*		
			database*		
			table*		
BatchDeleteTable	Gewährt die Berechtigung zum Löschen einer oder mehrerer Tabellen.	Write	catalog*		
			database*		
			table*		
BatchDeleteTableVersion	Gewährt die Berechtigung zum Löschen einer oder mehrerer Versionen einer Tabelle.	Schreiben	catalog*		
			database*		
			table*		
BatchGetBlueprints	Gewährt die Berechtigung zum Abrufen eines oder mehrerer Vorlagen	Lesen	blueprint*		
BatchGetCrawlers	Gewährt die Berechtigung zum Abrufen eines oder mehrerer Crawler.	Lesen	crawler*		
BatchGetCustomEntityTypes	Gewährt die Berechtigung zum Abrufen eines oder mehrerer benutzerdefinierter Entitätstypen	Lesen	customEntityType*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetDevEndpoints	Gewährt die Berechtigung zum Abrufen eines oder mehrerer Entwicklungsendpunkte.	Read	devendpoint*		
BatchGetJobs	Gewährt die Berechtigung zum Abrufen eines oder mehrerer Aufträge.	Read	job*		
BatchGetPartition	Gewährt die Berechtigung zum Abrufen einer oder mehrerer Partitionen.	Lesen	catalog*		
			database*		
			table*		
BatchGetStageFiles	Erteilt die Berechtigung zum Batch-Abrufen von Staging-Dateien für SparkUI	Berechtigungsverwaltung			
BatchGetTableOptimizer	Gewährt die Berechtigung zum Zurückgeben der Konfiguration für die angegebenen Tabellenoptimierer	Lesen	catalog*		glue:GetTable
			database*		
			table*		
BatchGetTriggers	Gewährt die Berechtigung zum Abrufen eines oder mehrerer Auslöser.	Read	trigger*		
BatchGetWorkflows	Gewährt die Berechtigung zum Abrufen eines oder mehrerer Workflows.	Read	workflow*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchStopJobRun	Gewährt die Berechtigung zum Anhalten einer oder mehrerer Auftragsausführungen für einen Auftrag.	Schreiben	job*		
BatchUpdatePartition	Gewährt die Berechtigung zum Aktualisieren einer oder mehrerer Partitionen	Schreiben	catalog*		
			database*		
			table*		
CancelDataQualityRuleRecommendationRun	Gewährt die Berechtigung zum Beenden einer laufenden Datenqualitätsregel	Schreiben	dataQualityRuleset*		
CancelDataQualityRulesetEvaluationRun	Gewährt die Berechtigung zum Beenden eines laufenden Datenqualitätsregelsatzes	Schreiben	dataQualityRuleset*		
CancelMLTaskRun	Gewährt die Berechtigung zum Beenden einer aktiven ML-Aufgabenausführung.	Schreiben	mlTransform*		
CancelStatement	Gewährt die Berechtigung zum Abbrechen einer Erklärung in einer interaktiven Sitzung	Schreiben	session*		
CheckSchemaVersionValidity	Gewährt die Berechtigung zum Abrufen einer Überprüfung der Gültigkeit der Schemaversion	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateBlueprint	Gewährt die Berechtigung zum Erstellen einer Vorlage	Schreiben	blueprint*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClassifier	Gewährt die Berechtigung zum Erstellen eines Classifiers.	Write			
CreateConnection	Gewährt die Berechtigung zum Erstellen einer Verbindung.	Write	catalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCrawler	Gewährt die Berechtigung zum Erstellen eines Crawlers.	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCustomEntityType	Gewährt die Berechtigung zum Erstellen eines benutzerdefinierten Entitätstyps	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataQualityRuleset	Gewährt die Berechtigung zum Erstellen eines Regelsatzes für die Datenqualität	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDatabase	Gewährt die Berechtigung zum Erstellen einer Datenbank.	Write	catalog* database*		
CreateDevEndpoint	Gewährt die Berechtigung zum Erstellen eines Entwicklungsendpunkts.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateJob	Gewährt die Berechtigung zum Erstellen eines Auftrags.	Write	job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys glue:VpcIds glue:SubnetIds glue:SecurityGroupIds	
CreateMLTransform	Gewährt die Berechtigung zum Erstellen einer ML-Transformation.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePartition	Gewährt die Berechtigung zum Erstellen einer Partition.	Schreiben	catalog*		
			database*		
			table*		
CreatePartitionIndex	Gewährt die Berechtigung zum Erstellen eines angegebenen Partitionsindex in einer vorhandenen Tabelle	Schreiben	catalog*		
			database*		
			table*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateRegistry	Gewährt die Berechtigung zum Erstellen einer neuen Schemaregistrierung	Write	registry*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSchema	Gewährt die Berechtigung zum Erstellen eines neuen Schemacontainers	Write	registry*		
			schema*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScript	Gewährt die Berechtigung zum Erstellen eines Skripts.	Write			
CreateSecurityConfiguration	Gewährt die Berechtigung zum Erstellen einer Sicherheitskonfiguration.	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSession	Gewährt die Berechtigung zum Erstellen einer interaktiven Sitzung	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys glue:VpcIds glue:SubnetIds glue:SecurityGroupIds	
CreateTable	Gewährt die Berechtigung zum Erstellen einer Tabelle.	Schreiben	catalog*		
			database*		
			table*		
CreateTableOptimizer	Gewährt die Berechtigung zum Erstellen eines neuen Tabellenoptimierers für eine bestimmte Funktion. Komprimierung ist der einzige derzeit unterstützte Optimierertyp	Schreiben	catalog*		glue:GetTable
			database*		
			table*		
CreateTrigger	Gewährt die Berechtigung zum Erstellen eines Auslösers.	Write	trigger*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUserDefinedFunction	Gewährt die Berechtigung zum Erstellen einer Funktionsdefinition.	Write	catalog*		
			database*		
CreateWorkflow	Gewährt die Berechtigung zum Erstellen eines Workflows	Schreiben	workflow*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBlueprint	Gewährt die Berechtigung zum Löschen einer Vorlage	Schreiben	blueprint*		
DeleteClassifier	Gewährt die Berechtigung zum Löschen eines Classifiers.	Schreiben			
DeleteColumnStatisticsForPartition	Gewährt die Berechtigung zum Löschen der Partitionsspaltenstatistiken einer Spalte	Schreiben	catalog*		
			database*		
			table*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteColumnStatisticsForTable	Gewährt die Berechtigung zum Löschen der Tabellenstatistiken von Spalten	Schreiben	catalog*		
			database*		
			table*		
DeleteConnection	Gewährt die Berechtigung zum Löschen einer Verbindung.	Write	catalog*		
			connection*		
DeleteCrawler	Gewährt die Berechtigung zum Löschen eines Crawlers.	Schreiben	crawler*		
DeleteCustomEntityType	Gewährt die Berechtigung zum Löschen eines benutzerdefinierten Entitätstyps	Schreiben	customEntityType*		
DeleteDataQualityRuleset	Gewährt die Berechtigung zum Löschen eines Regelsatzes für die Datenqualität	Schreiben	dataQualityRuleset*		
DeleteDatabase	Gewährt die Berechtigung zum Löschen einer Datenbank.	Write	catalog*		
			database*		
			table*		
			userdefinedfunction*		
DeleteDevEndpoint	Gewährt die Berechtigung zum Löschen eines Entwicklungsendpunkts.	Write	devendpoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteJob	Gewährt die Berechtigung zum Löschen eines Auftrags.	Write	job*		
DeleteMLTransform	Gewährt die Berechtigung zum Löschen einer ML-Transformation.	Write	mlTransform*		
DeletePartition	Gewährt die Berechtigung zum Löschen einer Partition.	Schreiben	catalog*		
			database*		
			table*		
DeletePartitionIndex	Gewährt die Berechtigung zum Löschen eines angegebenen Partitionsindex in einer vorhandenen Tabelle	Schreiben	catalog*		
			database*		
			table*		
DeleteRegistry	Gewährt die Berechtigung zum Löschen einer Schemaregistrierung	Write	registry*		
DeleteResourcePolicy	Gewährt die Berechtigung zum Löschen einer Ressourcenrichtlinie.	Berechtigungsverwaltung	catalog*		
DeleteSchema	Gewährt die Berechtigung zum Löschen eines Schemacontainers	Write	registry*		
			schema*		
DeleteSchemaVersions	Gewährt die Berechtigung zum Löschen eines Bereichs von Schemaversionen	Write	registry*		
			schema*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteSecurityConfiguration	Gewährt die Berechtigung zum Löschen einer Sicherheitskonfiguration.	Schreiben			
DeleteSession	Gewährt die Berechtigung zum Löschen einer interaktiven Sitzung nach Beendigung der Sitzung, wenn sie noch nicht gestoppt wurde	Schreiben	session*		
DeleteTable	Gewährt die Berechtigung zum Löschen einer Tabelle.	Schreiben	catalog*		
			database*		
			table*		
DeleteTableOptimizer	Gewährt die Berechtigung zum Löschen eines Optimierers und aller zugehörigen Metadaten für eine Tabelle. Die Optimierung wird nicht mehr an der Tabelle durchgeführt	Schreiben	catalog*		glue:GetTable
			database*		
			table*		
DeleteTableVersion	Gewährt die Berechtigung zum Löschen einer Version einer Tabelle.	Write	catalog*		
			database*		
			table*		
DeleteTrigger	Gewährt die Berechtigung zum Löschen eines Auslösers.	Write	trigger*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteUserDefinedFunction	Gewährt die Berechtigung zum Löschen einer Funktionsdefinition.	Write	catalog*		
			database*		
			userdefinedfunction*		
DeleteWorkflow	Gewährt die Berechtigung zum Löschen eines Workflows	Schreiben	workflow*		
DeregisterDataPreview	Gewährt die Berechtigung zum Beenden einer Glue-Studio-Notebook-Sitzung	Berechtigungsverwaltung			
GetBlueprint	Gewährt die Berechtigung zum Abrufen einer Vorlage	Lesen	blueprint*		
GetBlueprintRun	Gewährt die Berechtigung zum Abrufen einer Vorlagenausführung	Lesen	blueprint*		
GetBlueprintRuns	Gewährt die Berechtigung zum Abrufen aller Ausführungen von Vorlagen	Lesen	blueprint*		
GetCatalogImportStatus	Gewährt die Berechtigung zum Abrufen des Katalogimportstatus.	Read	catalog*		
GetClassifier	Gewährt die Berechtigung zum Abrufen eines Classifiers.	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetClassifiers	Gewährt die Berechtigung zum Auflisten aller Classifier.	Lesen			
GetColumnStatisticsForPartition	Gewährt die Berechtigung zum Abrufen von Partitionsstatistiken von Spalten	Lesen	catalog*		
			database*		
			table*		
GetColumnStatisticsForTable	Gewährt die Berechtigung zum Abrufen der Tabellenstatistiken von Spalten	Lesen	catalog*		
			database*		
			table*		
GetColumnStatisticsTaskRun	Gewährt die Berechtigung zum Abrufen der Ausführungsinformationen von Column Statistics für die Tabelle auf der Grundlage der run-id	Lesen			
GetColumnStatisticsTaskRuns	Gewährt die Berechtigung zum Abrufen der Ausführungsinformationen von Column Statistics für die Tabelle auf der Grundlage der run-ids	Lesen			
GetCompletion	Erteilt die Erlaubnis, eine generierte Antwort auf eine Fertigstellungsanfrage in Glue von AWS Q zu erhalten	Lesen	completion*		
GetConnection		Read	catalog*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Gewährt die Berechtigung zum Abrufen einer Verbindung.		connection*		
GetConnections	Gewährt die Berechtigung zum Abrufen einer Liste von Verbindungen	Read	catalog*		
			connection*		
GetCrawler	Gewährt die Berechtigung zum Abrufen eines Crawlers.	Read	crawler*		
GetCrawlerMetrics	Gewährt die Berechtigung zum Abrufen von Metriken über Crawler.	Read			
GetCrawlers	Gewährt die Berechtigung zum Abrufen aller Crawler.	Lesen			
GetCustomEntityType	Gewährt die Berechtigung zum Lesen eines benutzerdefinierten Entitätstyps	Lesen	customEntityType*		
GetDataCatalogEncryptionSettings	Gewährt die Berechtigung zum Abrufen von Katalogverschlüsselungseinstellungen.	Lesen	catalog*		
GetDataPreviewStatement	Gewährt die Berechtigung zum Abrufen einer Datenvorschau-Anweisung	Berechtigungsverwaltung			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDataQualityResult	Gewährt die Berechtigung zum Abrufen eines Datenqualitätsergebnisses	Lesen	dataQualityRuleset*		
GetDataQualityRuleRecommendationRun	Gewährt die Berechtigung zum Abrufen einer Datenqualitätsregel	Lesen	dataQualityRuleset*		
GetDataQualityRuleset	Gewährt die Berechtigung zum Abrufen eines Regelsatzes für die Datenqualität	Lesen	dataQualityRuleset*		
GetDataQualityRulesetEvaluationRun	Gewährt die Berechtigung zum Abrufen einer Datenqualitätsregel	Lesen	dataQualityRuleset*		
GetDatabase	Gewährt die Berechtigung zum Abrufen einer Datenbank.	Read	catalog* database*		
GetDatabases	Gewährt die Berechtigung zum Abrufen aller Datenbanken.	Read	catalog* database*		
GetDataflowGraph	Gewährt die Berechtigung zum Transformieren eines Skripts in ein azyklisch gerichtetes Diagramm (DAG).	Read			
GetDevEndpoint	Gewährt die Berechtigung zum Abrufen eines Entwicklungsendpunkts.	Read	devendpoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDevEndpoints	Gewährt die Berechtigung zum Abrufen aller Entwicklungsendpunkte.	Lesen			
GetEnvironment	Erteilt die Erlaubnis, Umgebungsdetails für SparkUI abzurufen	Berechtigungsverwaltung			
GetExecutors	Erteilt die Erlaubnis, Executoren für SparkUI zu finden	Berechtigungsverwaltung			
GetExecutorsThreads	Erteilt die Erlaubnis, Executor-Threads für SparkUI abzurufen	Berechtigungsverwaltung			
GetJob	Gewährt die Berechtigung zum Abrufen eines Auftrags.	Read	job*		
GetJobBookmark	Gewährt die Berechtigung zum Abrufen eines Auftragslesezeichens.	Read			
GetJobRun	Gewährt die Berechtigung zum Abrufen einer Auftragsausführung.	Read	job*		
GetJobRuns	Gewährt die Berechtigung zum Abrufen aller Auftragsausführungen eines Auftrags.	Read	job*		
GetJobs	Gewährt die Berechtigung zum Abrufen aller aktuellen Aufträge.	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetLogParsingStatus	Erteilt die Erlaubnis, den Log-Parsing-Status für SparkUI abzurufen	Berechtigungsverwaltung			
GetMLTaskRun	Gewährt die Berechtigung zum Abrufen einer ML-Aufgabenausführung.	Read	mlTransform*		
GetMLTaskRuns	Gewährt die Berechtigung zum Abrufen aller ML-Aufgabenausführungen.	List	mlTransform*		
GetMLTransform	Gewährt die Berechtigung zum Abrufen einer ML-Transformation.	Read	mlTransform*		
GetMLTransforms	Gewährt die Berechtigung zum Abrufen aller ML-Transformationen.	List	mlTransform*		
GetMapping	Gewährt die Berechtigung zum Erstellen einer Mapping.	Lesen			
GetNotebookInstanceStatus	Gewährt die Berechtigung zum Abrufen des Sitzungsstatus von Glue Studio Notebooks	Berechtigungsverwaltung			
GetPartition	Gewährt die Berechtigung zum Abrufen einer Partition.	Lesen	catalog*		
			database*		
			table*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetPartitionIndexes	Gewährt die Berechtigung zum Abrufen von Partitionsindizes für eine Tabelle	Lesen	catalog*		
			database*		
			table*		
GetPartitions	Gewährt die Berechtigung zum Abrufen der Partitionen einer Tabelle.	Read	catalog*		
			database*		
			table*		
GetPlan	Gewährt die Berechtigung zum Abrufen einer Mapping für ein Skript.	Lesen			
GetQueries	Erteilt die Erlaubnis, Abfragen für SparkUI abzurufen	Berechtigungsverwaltung			
GetQuery	Erteilt die Erlaubnis, eine bestimmte Abfrage für SparkUI abzurufen	Berechtigungsverwaltung			
GetRegistry	Gewährt die Berechtigung zum Abrufen einer Schemaregistrierung	Read	registry*		
GetResourcePolicies	Gewährt die Berechtigung zum Abrufen von Ressourcenrichtlinien	Read	catalog*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetResourcePolicy	Gewährt die Berechtigung zum Abrufen einer Ressourcenrichtlinie.	Read	catalog*		
GetSchema	Gewährt die Berechtigung zum Abrufen eines Schemacontainers	Read	registry*		
			schema*		
GetSchemaByDefinition	Gewährt die Berechtigung zum Abrufen einer Schemaversion basierend auf der Schemadefinition	Read	registry*		
			schema*		
GetSchemaVersion	Gewährt die Berechtigung zum Abrufen einer Schemaversion	Read	registry		
			schema		
GetSchemaVersionsDiff	Gewährt die Berechtigung, zwei Schemaversionen in der Schemaregistrierung zu vergleichen	Read	registry*		
			schema*		
GetSecurityConfiguration	Gewährt die Berechtigung zum Abrufen einer Sicherheitskonfiguration.	Read			
GetSecurityConfigurations	Gewährt die Berechtigung zum Abrufen einer oder mehrerer Sicherheitskonfigurationen.	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetSession	Gewährt die Berechtigung zum Abrufen einer interaktiven Sitzung	Lesen	session*		
GetStage	Erteilt die Erlaubnis, eine Stufe für SparkUI zu erstellen	Berechtigungsverwaltung			
GetStageAttempt	Erteilt die Erlaubnis, einen Stufenversuch für SparkUI zu starten	Berechtigungsverwaltung			
GetStageAttemptTaskList	Erteilt die Erlaubnis, die Aufgabenliste für einen Stufenversuch für SparkUI abzurufen	Berechtigungsverwaltung			
GetStageAttemptTaskSummary	Erteilt die Berechtigung, die Aufgabenzusammenfassung für einen Stufenversuch für SparkUI abzurufen	Berechtigungsverwaltung			
GetStageFiles	Erteilt die Erlaubnis, Staging-Dateien für SparkUI abzurufen	Berechtigungsverwaltung			
GetStages	Erteilt die Erlaubnis, Stufen für SparkUI abzurufen	Berechtigungsverwaltung			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetStatement	Gewährt die Berechtigung zum Abrufen von Ergebnissen und Informationen über eine Anweisung in einer interaktiven Sitzung	Lesen	session*		
GetStorage	Erteilt die Erlaubnis, Speicherdetails für SparkUI abzurufen	Berechtigungsverwaltung			
GetStorageUnit	Erteilt die Erlaubnis, Details zur Speichereinheit für SparkUI abzurufen	Berechtigungsverwaltung			
GetTable	Gewährt die Berechtigung zum Abrufen einer Tabelle.	Lesen	catalog*		
			database*		
			table*		
GetTableOptimizer	Gewährt die Berechtigung zum Zurückgeben der Konfiguration aller Optimierer, die einer angegebenen Tabelle zugeordnet sind	Lesen	catalog*		glue:GetTable
			database*		
			table*		
GetTableVersion	Gewährt die Berechtigung zum Abrufen einer Version einer Tabelle.	Read	catalog*		
			database*		
			table*		
GetTableVersions		Read	catalog*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Gewährt die Berechtigung zum Abrufen einer Liste der Versionen einer Tabelle		database*		
			table*		
GetTables	Gewährt die Berechtigung zum Abrufen der Tabellen in einer Datenbank.	Read	catalog*		
			database*		
			table*		
GetTags	Gewährt die Berechtigung zum Abrufen aller Tags, die einer Ressource zugeordnet sind.	Read	blueprint		
			crawler		
			customEntityType		
			devendpoint		
			job		
			trigger		
			workflow		
GetTrigger	Gewährt die Berechtigung zum Abrufen eines Auslösers.	Read	trigger*		
GetTriggers	Gewährt die Berechtigung zum Abrufen der Auslöser, die einem Auftrag zugeordnet sind.	Lesen			
GetUserDefinedFunction		Lesen	catalog*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Gewährt die Berechtigung zum Abrufen einer Funktionsdefinition		database*		
			userdefinedfunction*		
GetUserDefinedFunctions	Gewährt die Berechtigung zum Abrufen mehrerer Funktionsdefinitionen.	Read	catalog*		
			database*		
			userdefinedfunction*		
GetWorkflow	Gewährt die Berechtigung zum Abrufen eines Workflows.	Read	workflow*		
GetWorkflowRun	Gewährt die Berechtigung zum Abrufen einer Workflowausführung	Read	workflow*		
GetWorkflowRunProperties	Gewährt die Berechtigung zum Abrufen von Workflowausführungseigenschaften	Read	workflow*		
GetWorkflowRuns	Gewährt die Berechtigung zum Abrufen aller Ausführungen eines Workflows.	Lesen	workflow*		
GlueNotebookAuthorize	Gewährt die Berechtigung zum Zugreifen auf Glue Studio Notebooks	Berechtigungsverwaltung			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GlueNotebookRefreshCredentials	Gewährt die Berechtigung zum Aktualisieren der Anmeldeinformationen von Glue Studio Notebooks	Berechtigungsverwaltung			
ImportCatalogToGlue	Erteilt die Erlaubnis, einen Athena-Datenkatalog in AWS Glue zu importieren	Schreiben	catalog*		
ListBlueprints	Gewährt die Berechtigung zum Abrufen aller Vorlagen	Auflisten			
ListColumnStatisticsTaskRuns	Gewährt die Berechtigung zum Auflisten aller run-ids für Column Statistics, die für das Konto ausgeführt wurden	Lesen			
ListCrawlers	Gewährt die Berechtigung zum Abrufen aller Crawler.	Auflisten			
ListCrawls	Gewährt die Berechtigung zum Abrufen des Crawl-Ausführungsverlaufs für einen Crawler	Auflisten			
ListCustomEntityTypes	Gewährt die Berechtigung zum Abrufen aller benutzerdefinierter Entitätstypen	Auflisten			
ListDataQualityResults	Gewährt die Berechtigung zum Abrufen aller Datenqualitätsergebnisse	Auflisten	dataQualityRuleset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDataQualityRulesetRecommendationRuns	Gewährt die Berechtigung zum Abrufen aller Ausführungen von Datenqualitätsregeln	Auflisten	dataQualityRuleset*		
ListDataQualityRulesetEvaluationRuns	Gewährt die Berechtigung zum Abrufen aller Ausführungen von Datenqualitätsregeln	Auflisten	dataQualityRuleset*		
ListDataQualityRulesets	Gewährt die Berechtigung zum Abrufen einer Liste von Regelsätzen für die Datenqualität	Auflisten	dataQualityRuleset*		
ListDevEndpoints	Gewährt die Berechtigung zum Abrufen aller Entwicklungsendpunkte.	List			
ListJobs	Gewährt die Berechtigung zum Abrufen aller aktuellen Aufträge.	List			
ListMLTransforms	Gewährt die Berechtigung zum Abrufen aller ML-Transformationen.	List	mlTransform*		
ListRegistries	Gewährt die Berechtigung zum Abrufen einer Liste von Schemaregistrierungen	List			
ListSchemaVersions		List	registry*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Gewährt die Berechtigung zum Abrufen einer Liste von Schemaversionen		schema*		
ListSchemas	Gewährt die Berechtigung zum Abrufen einer Liste von Schemacontainern	Auflisten	registry		
ListSessions	Gewährt die Berechtigung zum Abrufen einer Liste interaktiver Sitzungen	Auflisten			
ListStatements	Gewährt die Berechtigung zum Abrufen einer Liste von Erklärungen in einer interaktiven Sitzung	Auflisten	session*		
ListTableOptimizerRuns	Gewährt die Berechtigung zum Auflisten des Verlaufs früherer Optimiererausführungen für eine bestimmte Tabelle	Auflisten	catalog*		glue:GetTable
			database*		
			table*		
ListTriggers	Gewährt die Berechtigung zum Abrufen aller Auslöser.	List			
ListWorkflows	Gewährt die Berechtigung zum Abrufen aller Workflows.	Auflisten			
NotifyEvent	Gewährt die Berechtigung, ein Ereignis an den ereignisgesteuerten Workflow zu benachrichtigen	Schreiben	workflow*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PassConnection [nur Berechtigung]	Gewährt die Berechtigung zum Übergeben des Namens der Glue-Verbindung in der Eingabe für APIs, die diese benötigen	Schreiben	connection*		
PublishDataQuality [nur Berechtigung]	Gewährt die Berechtigung zum Veröffentlichen von Datenqualitätsergebnissen	Schreiben	dataQualityRuleset*		
PutDataCatalogEncryptionSettings	Gewährt die Berechtigung zum Aktualisieren von Katalogverschlüsselungseinstellungen.	Write	catalog*		
PutResourcePolicy	Gewährt die Berechtigung zum Aktualisieren einer Ressourcenrichtlinie.	Berechtigungsverwaltung	catalog*		
PutSchemaVersionMetadata	Gewährt die Berechtigung zum Hinzufügen von Metadaten zu einer Schemaversion	Write	registry		
			schema		
PutWorkflowRunProperties	Gewährt die Berechtigung zum Aktualisieren von Workflowausführungseigenschaften	Write	workflow*		
QuerySchemaVersionMetadata	Gewährt die Berechtigung zum Abrufen von Metadaten für eine Schemaversion	List	registry		
			schema		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RegisterSchemaVersion	Gewährt die Berechtigung zum Erstellen einer neuen Schemaversion	Write	registry*		
			schema*		
RemoveSchemaVersionMetadata	Gewährt die Berechtigung zum Entfernen von Metadaten aus einer Schemaversion	Schreiben	registry		
			schema		
RequestLogParsing	Erteilt die Erlaubnis, die Protokollanalyse für SparkUI anzufordern	Berechtigungsverwaltung			
ResetJobBookmark	Gewährt die Berechtigung zum Zurücksetzen eines Auftragslesezeichens.	Write			
ResumeWorkflowRun	Gewährt die Berechtigung zum Fortsetzen einer Workflowausführung	Schreiben	workflow*		
RunDataPreviewStatement	Gewährt die Berechtigung zum Ausführen einer Datenvorschau-Anweisung	Berechtigungsverwaltung			
RunStatement	Gewährt die Berechtigung zum Ausführen eines Codes oder einer Erklärung in einer interaktiven Sitzung	Schreiben	session*		
SearchTables	Gewährt die Berechtigung zum Abrufen der Tabellen in einem Katalog.	Lesen	catalog*		
			database*		
			table*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SendFeedback	Erteilt die Erlaubnis, Feedback zu einer Erfahrung mit der Fertigstellung von Glue in Q zu geben AWS	Schreiben			
StartBlueprintRun	Gewährt die Berechtigung zum Starten der Ausführung einer Vorlage	Schreiben	blueprint*		
StartColumnStatisticsTaskRun	Gewährt die Berechtigung zum Starten einer Ausführung zum Generieren von Column Statistics für die Tabelle	Schreiben	database*		glue:GetSecurityConfiguration glue:GetTable
			table*		
StartCompletion	Erteilt die Erlaubnis, eine Fertigstellungsanfrage in Glue for AWS Q Experience zu erstellen	Schreiben			
StartCrawler	Gewährt die Berechtigung zum Starten eines Crawlers.	Write	crawler*		
StartCrawlerSchedule	Gewährt die Berechtigung zum Ändern des Planungsstatus eines Crawlers in SCHEDULED (GEPLANT).	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartDataQualityRuleRecommendationRun	Gewährt die Berechtigung zum Starten einer Vorlagenausführung von Datenqualitätsregeln	Schreiben	dataQualityRuleset*		
StartDataQualityRulesetEvaluationRun	Gewährt die Berechtigung zum Starten einer Vorlagenausführung von Datenqualitätsregeln	Schreiben	dataQualityRuleset*		
StartExportLabelsTaskRun	Gewährt die Berechtigung zum Starten einer ML-Aufgabenausführung zum Exportieren von Labels.	Write	mlTransform*		
StartImportLabelsTaskRun	Gewährt die Berechtigung zum Starten einer ML-Aufgabenausführung zum Importieren von Labels.	Write	mlTransform*		
StartJobRun	Gewährt die Berechtigung zum Starten eines Auftrags.	Write	job*		
StartMLEvaluationTaskRun	Gewährt die Berechtigung zum Starten einer ML-Aufgabenausführung zum Evaluieren.	Write	mlTransform*		
StartMLLabelingSetGenerationTaskRun	Gewährt die Berechtigung zum Starten einer ML-Aufgabenausführung zum Generieren eines Label-Sets.	Schreiben	mlTransform*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartNotebook	Gewährt die Berechtigung zum Starten von Glue Studio Notebooks	Berechtigungsverwaltung			
StartTrigger	Gewährt die Berechtigung zum Starten eines Auslösers.	Write	trigger*		
StartWorkflowRun	Gewährt die Berechtigung zum Starten eines Workflows.	Schreiben	workflow*		
StopColumnStatisticsTaskRun	Gewährt die Berechtigung zum Stoppen der Ausführung von Column Statistics	Schreiben	database* table*		
StopCrawler	Gewährt die Berechtigung zum Beenden eines aktiven Crawlers.	Write	crawler*		
StopCrawlerSchedule	Gewährt die Berechtigung zum Festlegen des Planungsstatus eines Crawlers auf NOT_SCHEDULED (NICHT_GEPLANT).	Schreiben			
StopSession	Gewährt die Berechtigung zum Anhalten einer interaktiven Sitzung	Schreiben	session*		
StopTrigger	Gewährt die Berechtigung zum Stoppen eines Auslösers.	Write	trigger*		
StopWorkflowRun	Gewährt die Berechtigung zum Stoppen einer Workflowausführung	Write	workflow*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Ressource	Tagging	blueprint		
			connection		
			crawler		
			customEntityType		
			dataQualityRuleset		
			devendpoint		
			job		
			mlTransform		
			registry		
			schema		
			session		
			trigger		
			workflow		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
TerminateNotebook	Gewährt die Berechtigung zum Beenden von Glue Studio Notebooks	Berechtigungsverwaltung			
TestConnection	Gewährt die Berechtigung zum Testen der Verbindung in Glue Studio	Berechtigungsverwaltung			
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags, die einer Ressource zugeordnet sind.	Tagging	blueprint		
			connection		
			crawler		
			customEntityType		
			dataQualityRuleset		
			devendpoint		
			job		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			mlTransform		
			registry		
			schema		
			session		
			trigger		
			workflow		
				aws:TagKeys	
UpdateBlueprint	Gewährt die Berechtigung zum Aktualisieren einer Vorlage	Schreiben	blueprint*		
UpdateClassifier	Gewährt die Berechtigung zum Aktualisieren eines Classifiers.	Schreiben			
UpdateColumnStatisticsForPartition	Gewährt die Berechtigung zum Aktualisieren von Partitionsstatistiken von Spalten	Schreiben	catalog*		
			database*		
			table*		
UpdateColumnStatisticsForTable	Gewährt die Berechtigung zum Aktualisieren der Tabellenstatistiken von Spalten	Schreiben	catalog*		
			database*		
			table*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateConnection	Gewährt die Berechtigung zum Aktualisieren einer Verbindung.	Write	catalog*		
			connection*		
UpdateCrawler	Gewährt die Berechtigung zum Aktualisieren eines Crawlers.	Write	crawler*		
UpdateCrawlerSchedule	Gewährt die Berechtigung zum Aktualisieren des Zeitplans eines Crawlers.	Schreiben			
UpdateDataQualityRuleset	Gewährt die Berechtigung zum Aktualisieren eines Regelsatzes für die Datenqualität	Schreiben	dataQualityRuleset*		
UpdateDatabase	Gewährt die Berechtigung zum Aktualisieren einer Datenbank.	Write	catalog*		
			database*		
UpdateDevEndpoint	Gewährt die Berechtigung zum Aktualisieren eines Entwicklungsendpunkts.	Write	devendpoint*		
UpdateJob	Gewährt die Berechtigung zum Aktualisieren eines Auftrags.	Schreiben	job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				glue:VpcIds glue:SubnetIds glue:SecurityGroupIds	
UpdateJobFromSourceControl	Gewährt die Berechtigung zum Aktualisieren eines Auftrags über den Quellsteuerungsanbieter	Schreiben	job*		
UpdateMLTransform	Gewährt die Berechtigung zum Aktualisieren einer ML-Transformation.	Write	mlTransform*		
UpdatePartition	Gewährt die Berechtigung zum Aktualisieren einer Partition.	Write	catalog*		
			database*		
			table*		
UpdateRegistry	Gewährt die Berechtigung zum Aktualisieren einer Schemaregistrierung	Write	registry*		
UpdateSchema	Gewährt die Berechtigung zum Aktualisieren eines Schemacontainers	Schreiben	registry*		
			schema*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateSourceControlFromJob	Gewährt die Berechtigung zum Aktualisieren des Quellsteuerungsanbieter über einen Auftrag	Schreiben	job*		
UpdateTable	Gewährt die Berechtigung zum Aktualisieren einer Tabelle.	Schreiben	catalog*		
			database*		
			table*		
UpdateTableOptimizer	Gewährt die Berechtigung zum Aktualisieren der Konfiguration für einen bestehenden Tabellenoptimierer	Schreiben	catalog*		glue:GetTable
			database*		
			table*		
UpdateTrigger	Gewährt die Berechtigung zum Aktualisieren eines Auslösers.	Write	trigger*		
UpdateUserDefinedFunction	Gewährt die Berechtigung zum Aktualisieren einer Funktionsdefinition.	Write	catalog*		
			database*		
			userdefinedfunction*		
UpdateWorkflow	Gewährt die Berechtigung zum Aktualisieren eines Workflows.	Schreiben	workflow*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UseGlueStudio	Gewährt die Berechtigung, Glue Studio zu verwenden und auf seine internen APIs zuzugreifen	Berechtigungsverwaltung			
UseMLTransforms [nur Berechtigung]	Gewährt die Berechtigung zur Verwendung einer ML-Transformation innerhalb eines Glue ETL-Skripts.	Write	mlTransform*		

Von AWS Glue definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
catalog	`arn:${Partition}:glue:${Region}:${Account}:catalog`	
database	`arn:${Partition}:glue:${Region}:${Account}:database/${DatabaseName}`	
table	`arn:${Partition}:glue:${Region}:${Account}:table/${DatabaseName}/${TableName}`	

Ressourcentypen	ARN	Bedingungsschlüssel
tableversion	arn:${Partition}:glue:${Region}:${Account}:tableVersion/${DatabaseName}/${TableName}/${TableVersionName}	
connection	arn:${Partition}:glue:${Region}:${Account}:connection/${ConnectionName}	aws:ResourceTag/${TagKey}
userdefinedfunction	arn:${Partition}:glue:${Region}:${Account}:userDefinedFunction/${DatabaseName}/${UserDefinedFunctionName}	
devendpoint	arn:${Partition}:glue:${Region}:${Account}:devEndpoint/${DevEndpointName}	aws:ResourceTag/${TagKey}
job	arn:${Partition}:glue:${Region}:${Account}:job/${JobName}	aws:ResourceTag/${TagKey}
trigger	arn:${Partition}:glue:${Region}:${Account}:trigger/${TriggerName}	aws:ResourceTag/${TagKey}
crawler	arn:${Partition}:glue:${Region}:${Account}:crawler/${CrawlerName}	aws:ResourceTag/${TagKey}
workflow	arn:${Partition}:glue:${Region}:${Account}:workflow/${WorkflowName}	aws:ResourceTag/${TagKey}
blueprint	arn:${Partition}:glue:${Region}:${Account}:blueprint/${BlueprintName}	aws:ResourceTag/${TagKey}
mlTransform	arn:${Partition}:glue:${Region}:${Account}:mlTransform/${TransformId}	aws:ResourceTag/${TagKey}
registry	arn:${Partition}:glue:${Region}:${Account}:registry/${RegistryName}	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
schema	arn:${Partition}:glue:${Region}:${Account}:schema/${SchemaName}	aws:ResourceTag/${TagKey}
session	arn:${Partition}:glue:${Region}:${Account}:session/${SessionId}	aws:ResourceTag/${TagKey}
dataQualityRuleset	arn:${Partition}:glue:${Region}:${Account}:dataQualityRuleset/${RulesetName}	aws:ResourceTag/${TagKey}
customEntityType	arn:${Partition}:glue:${Region}:${Account}:customEntityType/${CustomEntityTypeId}	aws:ResourceTag/${TagKey}
completion	arn:${Partition}:glue:${Region}:${Account}:completion/${CompletionId}	

Bedingungsschlüssel für AWS Glue

AWS Glue definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	String

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString
glue:CredentialIssuingService	Filtert den Zugriff nach dem Dienst, von dem die Anmeldeinformationen der Anforderung ausgegeben werden	String
glue:RoleAssumedBy	Filtert den Zugriff durch den Dienst, von dem die Anmeldeinformationen der Anforderung abgerufen werden, indem die Kundenrolle übernommen wird	String
glue:SecurityGroupIds	Filtert den Zugriff nach der ID von Sicherheitsgruppen, die für den Glue-Auftrag konfiguriert sind	ArrayOfString
glue:SubnetIds	Filtert den Zugriff anhand der ID von Subnetzen, die für den Glue-Auftrag konfiguriert sind	ArrayOfString
glue:VpcIds	Filtert den Zugriff anhand der ID der VPC, die für den Glue-Auftrag konfiguriert ist	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Glue DataBrew

AWS Glue DataBrew (Servicepräfix: `databrew`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Glue DataBrew definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchDeleteRecipeVersion	Gewährt die Berechtigung zum Löschen einer oder mehrerer Rezeptversionen	Write	Recipe*		
CreateDataset	Gewährt die Berechtigung zum Erstellen eines Dataset	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfileJob	Gewährt die Berechtigung zum Erstellen einer Profilaufgabe	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProject	Gewährt die Berechtigung zum Erstellen eines Projekts	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRecipe	Gewährt die Berechtigung zum Erstellen eines Rezepts	Write		aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
CreateRecipeJob	Gewährt die Berechtigung zum Erstellen einer Rezeptaufgabe	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleset	Gewährt die Berechtigung zum Erstellen eines Regelsatzes	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSchedule	Gewährt die Berechtigung zum Erstellen eines Zeitplans	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDataset	Gewährt die Berechtigung zum Löschen eines Dataset	Write	Dataset*		
DeleteJob	Gewährt die Berechtigung zum Löschen eines Auftrags.	Write	Job*		
DeleteProject	Gewährt die Berechtigung zum Löschen eines Projekts	Write	Project*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteRecipeVersion	Gewährt die Berechtigung zum Löschen einer Rezeptversion	Schreiben	Recipe*		
DeleteRuleset	Gewährt die Berechtigung zum Löschen eines Regelsatzes	Schreiben	Ruleset*		
DeleteSchedule	Gewährt die Berechtigung zum Löschen eines Zeitplans	Write	Schedule*		
DescribeDataset	Gewährt die Berechtigung zum Anzeigen von Details zu einem Dataset	Read	Dataset*		
DescribeJob	Gewährt die Berechtigung zum Anzeigen von Details zu einer Aufgabe	Read	Job*		
DescribeJobRun	Gewährt die Berechtigung zum Anzeigen von Details zum Job-Lauf für einen bestimmten Job	Read	Job*		
DescribeProject	Gewährt die Berechtigung zum Anzeigen von Details zu einem Projekt	Read	Project*		
DescribeRecipe	Gewährt die Berechtigung zum Anzeigen von Details zu einem Rezept	Lesen	Recipe*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeRuleset	Gewährt die Berechtigung zum Anzeigen von Details zu einem Regelsatz	Lesen	Ruleset*		
DescribeSchedule	Gewährt die Berechtigung zum Anzeigen von Details zu einem Zeitplan	Read	Schedule*		
ListDatasets	Gewährt die Berechtigung zum Auflisten von Datasets in Ihrem Konto	Read			
ListJobRuns	Gewährt die Berechtigung zum Auflisten von Ausführungen einer bestimmten Aufgabe	Read	Job*		
ListJobs	Gewährt die Berechtigung zum Auflisten von Aufgaben in Ihrem Konto	Read			
ListProjects	Gewährt die Berechtigung zum Auflisten von Projekten in Ihrem Konto	Read			
ListRecipeVersions	Gewährt die Berechtigung zum Auflisten von Versionen in Ihrem Rezept	Read	Recipe*		
ListRecipes	Gewährt die Berechtigung zum Auflisten von Rezepten in Ihrem Konto	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListRulesets	Gewährt die Berechtigung zum Auflisten von Regelsätzen in Ihrem Konto	Lesen			
ListSchedules	Gewährt die Berechtigung zum Auflisten von Zeitplänen in Ihrem Konto	Read			
ListTagsForResource	Gewährt die Berechtigung zum Abrufen von Tags, die einer Ressource zugeordnet sind	Read	Dataset		
			Job		
			Project		
			Recipe		
			Ruleset		
			Schedule		
PublishRecipe	Gewährt die Berechtigung, eine Hauptversion eines Rezepts zu veröffentlichen	Write	Recipe*		
SendProjectSessionAction	Gewährt die Berechtigung, eine Aktion an die interaktive Sitzung für ein Projekt zu senden	Write	Project*		
StartJobRun	Gewährt die Berechtigung zum Starten eines Auftrags.	Write	Job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartProjectSession	Gewährt die Berechtigung zum Starten einer interaktiven Sitzung für ein Projekt	Write	Project*		
StopJobRun	Gewährt die Berechtigung zum Anhalten einer Aufgabenausführung	Write	Job*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Ressource	Markieren	Dataset		
			Job		
			Project		
			Recipe		
			Ruleset		
			Schedule		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags, die einer Ressource zugeordnet sind.	Markieren	Dataset		
			Job		
			Project		
			Recipe		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			Ruleset		
			Schedule		
				aws:TagKeys	
UpdateDataset	Gewährt die Berechtigung zum Ändern eines Dataset	Write	Dataset*		
UpdateProfileJob	Gewährt die Berechtigung zum Ändern einer Profilaufgabe	Write	Job*		
UpdateProject	Gewährt die Berechtigung zum Ändern eines Projekts	Write	Project*		
UpdateRecipe	Gewährt die Berechtigung zum Ändern eines Rezepts	Write	Recipe*		
UpdateRecipeJob	Gewährt die Berechtigung zum Ändern einer Rezeptaufgabe	Schreiben	Job*		
UpdateRuleset	Gewährt die Berechtigung zum Ändern eines Regelsatzes	Schreiben	Ruleset*		
UpdateSchedule	Gewährt die Berechtigung zum Ändern eines Zeitplans	Write	Schedule*		

Von AWS Glue DataBrew definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Project	`arn:${Partition}:databrew:${Region}:${Account}:project/${ResourceId}`	aws:ResourceTag/${TagKey}
Dataset	`arn:${Partition}:databrew:${Region}:${Account}:dataset/${ResourceId}`	aws:ResourceTag/${TagKey}
Ruleset	`arn:${Partition}:databrew:${Region}:${Account}:ruleset/${ResourceId}`	aws:ResourceTag/${TagKey}
Recipe	`arn:${Partition}:databrew:${Region}:${Account}:recipe/${ResourceId}`	aws:ResourceTag/${TagKey}
Job	`arn:${Partition}:databrew:${Region}:${Account}:job/${ResourceId}`	aws:ResourceTag/${TagKey}
Schedule	`arn:${Partition}:databrew:${Region}:${Account}:schedule/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Glue DataBrew

AWS Glue DataBrew definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Ground Station.

AWS Ground Station (Servicepräfix: `groundstation`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Ground Station definierte Aktionen
- Von AWS Ground Station definierte Ressourcentypen
- Bedingungsschlüssel für AWS Ground Station

Von AWS Ground Station definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelContact	Gewährt die Berechtigung, einen Kontakt abzubrechen	Write	Contact*		
CreateConfig	Gewährt die Berechtigung zum Erstellen einer Konfiguration.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataflowEndpointGroup	Gewährt die Berechtigung zum Erstellen einer Datenfluss-Endpunktgruppe.	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateEphemeris	Gewährt die Berechtigung zum Erstellen eines Ephemeris-Elements	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMissionProfile	Gewährt die Berechtigung, ein Missionsprofil zu erstellen	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfig	Gewährt die Berechtigung zum Löschen einer Konfiguration.	Write	Config*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteDataflowEndpointGroup	Gewährt die Berechtigung zum Löschen einer Datenfluss-Endpunktgruppe.	Schreiben	DataflowEndpointGroup*		
DeleteEphemeris	Gewährt die Berechtigung zum Löschen eines Ephemeris-Elements	Schreiben	EphemerisItem*		
DeleteMissionProfile	Gewährt die Berechtigung zum Löschen eines Missionsprofils.	Write	MissionProfile*		
DescribeContact	Gewährt die Berechtigung, einen Kontakt zu beschreiben	Lesen	Contact*		
DescribeEphemeris	Gewährt die Berechtigung zum Beschreiben eines Ephemeris-Elements	Lesen	EphemerisItem*		
GetAgentConfiguration	Gewährt die Berechtigung zum Abrufen der Konfiguration eines Agenten	Lesen	Agent*		
GetConfig	Gewährt die Berechtigung zum Zurückgeben einer Konfiguration.	Read	Config*		
GetDataflowEndpointGroup	Gewährt die Berechtigung zum Zurückgeben einer Datenfluss-Endpunktgruppe.	Read	DataflowEndpointGroup*		
GetMinuteUsage	Gewährt die Berechtigung zum Zurückgeben der Minutennutzung.	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetMissionProfile	Gewährt die Berechtigung zum Abrufen eines Missionsprofils.	Read	MissionProfile*		
GetSatellite	Gewährt die Berechtigung zum Zurückgeben von Informationen zu einem Satelliten.	Read	Satellite*		
ListConfigs	Gewährt die Berechtigung zum Zurückgeben einer Liste der letzten Konfigurationen	List			
ListContacts	Gewährt die Berechtigung, eine Liste von Kontakten zurückzugeben	List			
ListDataflowEndpointGroups	Gewährt die Berechtigung zum Auflisten von Datenfluss-Endpunktgruppen.	Auflisten			
ListEphemerides	Gewährt die Berechtigung zum Auflisten von Ephemeriden	Auflisten			
ListGroundStations	Gewährt die Berechtigung zum Auflisten von Ground Stationen.	List			
ListMissionProfiles	Gewährt die Berechtigung zum Zurückgeben einer Liste der Missionsprofile.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListSatellites	Gewährt die Berechtigung zum Auflisten von Satelliten.	List			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen	Config		
			Contact		
			DataflowEndpointGroup		
			MissionProfile		
RegisterAgent	Gewährt die Berechtigung zum Registrieren eines Agenten	Schreiben			
ReserveContact	Gewährt die Berechtigung, einen Kontakt zu reservieren	Write		aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Gewährt die Berechtigung zum Zuordnen eines Ressourcen-Tags.	Markierung	Config		
			Contact		
			DataflowEndpointGroup		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			Ephemeris Item		
			MissionProfile		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen eines Ressourcen-Tags	Markierung	Config		
			Contact		
			DataflowEndpointGroup		
			Ephemeris Item		
			MissionProfile		
				aws:TagKeys	
UpdateAgentStatus	Gewährt die Berechtigung zum Aktualisieren des Namens eines Agenten	Schreiben	Agent*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateConfig	Gewährt die Berechtigung zum Aktualisieren einer Konfiguration.	Schreiben	Config*		
UpdateEphemeris	Gewährt die Berechtigung zum Aktualisieren eines Ephemeris-Elements	Schreiben	EphemerisItem*		
UpdateMissionProfile	Gewährt die Berechtigung, eine Missionsprofil zu aktualisieren	Write	MissionProfile*		

Von AWS Ground Station definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Config	`arn:${Partition}:groundstation:${Region}:${Account}:config/${ConfigType}/${ConfigId}`	aws:ResourceTag/${TagKey} groundstation:ConfigId groundstation:ConfigType

Ressourcentypen	ARN	Bedingungsschlüssel
Contact	arn:${Partition}:groundstation:${Region}:${Account}:contact/${ContactId}	aws:ResourceTag/${TagKey} groundstation:ContactId
DataflowEndpointGroup	arn:${Partition}:groundstation:${Region}:${Account}:dataflow-endpoint-group/${DataflowEndpointGroupId}	aws:ResourceTag/${TagKey} groundstation:DataflowEndpointGroupId
EphemerisItem	arn:${Partition}:groundstation:${Region}:${Account}:ephemeris/${EphemerisId}	aws:ResourceTag/${TagKey} groundstation:EphemerisId
GroundStationResource	arn:${Partition}:groundstation:${Region}:${Account}:groundstation:${GroundStationId}	groundstation:GroundStationId
MissionProfile	arn:${Partition}:groundstation:${Region}:${Account}:mission-profile/${MissionProfileId}	aws:ResourceTag/${TagKey} groundstation:MissionProfileId
Satellite	arn:${Partition}:groundstation:${Region}:${Account}:satellite/${SatelliteId}	groundstation:SatelliteId
Agent	arn:${Partition}:groundstation:${Region}:${Account}:agent/${AgentId}	groundstation:AgentId

Bedingungsschlüssel für AWS Ground Station

AWS Ground Station definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString
groundstation:AgentId	Filtert den Zugriff nach der ID eines Agenten	Zeichenfolge
groundstation:ConfigId	Filtert den Zugriff anhand der ID einer Konfiguration.	Zeichenfolge
groundstation:ConfigType	Filtert den Zugriff anhand des Typs einer Konfiguration.	Zeichenfolge
groundstation:ContactId	Filtert den Zugriff anhand der ID eines Kontakts.	Zeichenfolge
groundstation:DataflowEndpointGroupId	Filtert den Zugriff anhand der ID einer Datenfluss-Endpunktgruppe.	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
groundstation:EphemerisId	Filtert den Zugriff nach der ID eines Ephemeris	Zeichenfolge
groundstation:GroundStationId	Filtert den Zugriff anhand der ID einer Ground Station.	Zeichenfolge
groundstation:MissionProfileId	Filtert den Zugriff anhand der ID eines Missionsprofils.	Zeichenfolge
groundstation:SatelliteId	Filtert den Zugriff anhand der ID eines Satelliten.	Zeichenfolge

Aktionen, Ressourcen und Zustandsschlüssel für Amazon GroundTruth Labeling

Amazon GroundTruth Labeling (Servicepräfix:`groundtruthlabeling`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon GroundTruth Labeling definierte Aktionen
- Von Amazon GroundTruth Labeling definierte Ressourcentypen
- Zustandstasten für Amazon GroundTruth Labeling

Von Amazon GroundTruth Labeling definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociatePatchToManifestJob [nur Berechtigung]	Gewährt die Berechtigung zum Verknüpfen einer Patchdatei mit der Manifestdatei, um die Manifestdatei zu aktualisieren	Write			
CreateBatch [nur Berechtigung]	Erteilt die Erlaubnis, einen GT + Batch zu erstellen	Schreiben			
CreateIntakeForm [nur Berechtigung]	Erteilt die Erlaubnis zur Erstellung eines Aufnahmeformulars	Schreiben			
CreateProject [nur Berechtigung]	Erteilt die Erlaubnis, ein GT+-Projekt zu erstellen	Schreiben			
CreateWorkflowDefinition [nur Berechtigung]	Erteilt die Erlaubnis, eine GT+ Workflow-Definition zu erstellen	Schreiben			
DescribeConsoleJob [nur Berechtigung]	Erteilt die Erlaubnis, den Status von GroundTruthLabeling Jobs abzurufen	Lesen			
GenerateLIDARPreviewTaskConfigJob [nur Berechtigung]	Erteilt die Berechtigung zum Generieren einer LiDAR-Vorschauaufgabe	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBatch [nur Berechtigung]	Erteilt die Erlaubnis, einen GT + Batch zu erhalten	Lesen			
GetIntakeFormStatus [nur Berechtigung]	Erteilt die Erlaubnis, Aufnahmeformulare zu erhalten	Lesen			
ListBatches [nur Berechtigung]	Erteilt die Erlaubnis, GT+ Batchs aufzulisten	Lesen			
ListDatasetObjects [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Datensatz objekten in einer Manifestdatei	Read			
ListProjects [nur Berechtigung]	Erteilt die Erlaubnis, ein GT+-Projekt aufzulisten	Lesen			
RunFilterOrSampleDatasetJob [nur Berechtigung]	Gewährt die Berechtigung zum Filtern von Datensätzen aus einer Manifestdatei mit S3 Select. Anfordern von Beispieleinträgen basierend auf Stichproben	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RunGenerateManifestByCrawlingJob [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten eines S3-Präfix und Erstellen von Manifestdateien aus Objekten an diesem Speicherort	Schreiben			
RunGenerateManifestMetricsJob [nur Berechtigung]	Erteilt die Erlaubnis, Metriken aus Objekten im Manifest zu generieren	Schreiben			
UpdateBatch [nur Berechtigung]	Erteilt die Erlaubnis, einen GT + Batch zu aktualisieren	Schreiben			

Von Amazon GroundTruth Labeling definierte Ressourcentypen

Amazon GroundTruth Labeling unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource` Element einer IAM-Richtlinienerklärung. Um den Zugriff auf Amazon GroundTruth Labeling zu ermöglichen, geben Sie `"Resource": "*"` dies in Ihrer Richtlinie an.

Zustandstasten für Amazon GroundTruth Labeling

GroundTruth Für Labeling gibt es keine dienstspezifischen Kontextschlüssel, die `Condition` in Grundsatzerklärungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon GuardDuty

Amazon GuardDuty (Servicepräfix: `guardduty`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon GuardDuty definierte Aktionen
- Von Amazon GuardDuty definierte Ressourcentypen
- Bedingungsschlüssel für Amazon GuardDuty

Von Amazon GuardDuty definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptAdministratorInvitation	Gewährt die Berechtigung zum Akzeptieren von Einladungen, ein GuardDuty-Mitgliedskonto zu werden.	Schreiben			
AcceptInvitation	Gewährt die Berechtigung zum Akzeptieren von Einladungen, ein GuardDuty-Mitgliedskonto zu werden.	Write			
ArchiveFindings	Gewährt die Berechtigung zum Archivieren von GuardDuty-Ergebnissen.	Write			
CreateDetector	Gewährt die Berechtigung zum Erstellen eines Detektors.	Write		aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
CreateFilter	Gewährt die Berechtigung zum Erstellen von GuardDuty-Filtern. Ein Filter definiert Attribute und Bedingungen, die zum Filtern von Ergebnissen verwendet werden.	Write	filter*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIPSet	Gewährt die Berechtigung zum Erstellen eines IPSet.	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:DeleteRolePolicy iam:PutRolePolicy
CreateMembers	Gewährt die Berechtigung zum Erstellen von GuardDuty-Mitgliedskonten, wobei das zum Erstellen eines Mitglieds verwendete Konto zum GuardDuty-Administratorkonto wird	Write			
CreatePublishingDestination	Gewährt die Berechtigung zum Erstellen eines Veröffentlichungsziels.	Write			s3:GetObject s3:ListBucket

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSampleFindings	Gewährt die Berechtigung zum Erstellen von Beispielergebnissen.	Write			
CreateThreatIntelSet	Gewährt die Berechtigung zum Erstellen von GuardDuty ThreatIntelSets, wobei ein ThreatIntelSet aus bekannten schädlichen IP-Adressen besteht, die von GuardDuty zum Generieren von Ergebnissen verwendet werden	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeclineInvitations	Gewährt die Berechtigung zum Ablehnen von Einladungen, ein GuardDuty-Mitgliedskonto zu werden.	Write			
DeleteDetector	Gewährt die Berechtigung zum Löschen von GuardDuty-Detektoren.	Write	detector*		
DeleteFilter	Gewährt die Berechtigung zum Löschen von GuardDuty-Filtern.	Write	filter*		
DeleteIPSet	Gewährt die Berechtigung zum Löschen von GuardDuty-IPSets	Write	ipset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteInvitations	Gewährt die Berechtigung zum Löschen von Einladungen, ein GuardDuty-Mitgliedskonto zu werden.	Write			
DeleteMembers	Gewährt die Berechtigung zum Löschen von GuardDuty-Mitgliedskonten.	Write			
DeletePublishingDestination	Gewährt die Berechtigung zum Löschen eines Veröffentlichungsziels.	Write	publishingDestination*		
DeleteThreatIntelSet	Gewährt die Berechtigung zum Löschen von GuardDuty ThreatIntelSets.	Schreiben	threatintelset*		
DescribeMalwareScans	Erteilung der Berechtigung zum Abrufen von Details über Malware-Scans	Lesen			
DescribeOrganizationConfiguration	Gewährt die Berechtigung zum Abrufen von Details über den delegierten Administrator, der einem GuardDuty-Detektor zugeordnet ist.	Read			
DescribePublishingDestination	Gewährt die Berechtigung zum Abrufen von Details zu einem Veröffentlichungsziel.	Read	publishingDestination*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisableOrganizationAdminAccount	Gewährt die Berechtigung, den delegierten Organisationsadministrator für GuardDuty zu deaktivieren.	Schreiben			
DisassociateFromAdministratorAccount	Gewährt die Berechtigung zum Aufheben der Mapping eines GuardDuty-Mitgliedskontos zu seinem GuardDuty-Administratorkonto.	Schreiben			
DisassociateFromMasterAccount	Gewährt die Berechtigung zum Aufheben der Mapping eines GuardDuty-Mitgliedskontos zu seinem GuardDuty-Administratorkonto.	Schreiben			
DisassociateMembers	Gewährt die Berechtigung, die Mapping von GuardDuty-Mitgliedskonten zu ihrem GuardDuty-Konto aufzuheben	Schreiben			
EnableOrganizationAdminAccount	Gewährt die Berechtigung, einen delegierten Organisationsadministrator für GuardDuty zu aktivieren.	Schreiben			
GetAdministratorAccount	Gewährt die Berechtigung zum Abrufen von Details des GuardDuty-Administratorkontos, das einem Mitgliedskonto zugeordnet ist.	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetCoverageStatistics	Gewährt die Berechtigung zum Auflisten der Amazon GuardDuty-Nutzungsstatistiken für das angegebene GuardDuty-Konto in einer Region	Lesen	detector*		
GetDetector	Gewährt die Berechtigung zum Abrufen von GuardDuty-Detektoren.	Read	detector*		
GetFilter	Gewährt die Berechtigung zum Abrufen von GuardDuty-Filtern.	Read	filter*		
GetFindings	Gewährt die Berechtigung zum Abrufen von GuardDuty-Ergebnissen.	Read			
GetFindingsStatistics	Gewährt die Berechtigung zum Abrufen einer Liste von GuardDuty-Ergebnisstatistiken.	Lesen			
GetIPSet	Gewährt die Berechtigung zum Abrufen von GuardDuty-IPSets	Lesen	ipset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetInvitationsCount	Gewährt die Berechtigung zum Abrufen der Anzahl aller GuardDuty-Einladungen, die an ein bestimmtes Konto gesendet werden, enthält die angenommene Einladung nicht	Lesen			
GetMalwareScanSettings	Erteilung der Berechtigung zum Abrufen der Malware-Scaneinstellungen	Lesen			
GetMasterAccount	Gewährt die Berechtigung zum Abrufen von Details des GuardDuty-Administratorkontos, das einem Mitgliedskonto zugeordnet ist.	Lesen			
GetMemberDetectors	Gewährt die Berechtigung zu beschreiben, welche Datenquellen für Mitgliedkontendetektoren aktiviert sind	Lesen			
GetMembers	Gewährt die Berechtigung zum Abrufen der einem Administratorkonto zugeordneten Mitgliedskonten.	Lesen			
GetOrganizationStatistics	Gewährt die Genehmigung zum Abrufen von Deckungsstatistiken des GuardDuty-Schutzplans für Mitgliedskonten in einer Region	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetRemainingFreeTrialDays	Gewährt die Berechtigung zur Angabe der für jede im kostenlosen Testzeitraum verwendete Datenquelle verbleibenden Tage	Lesen			
GetThreatIntelSet	Gewährt die Berechtigung zum Abrufen von GuardDuty ThreatIntelSets.	Read	threatintelset*		
GetUsageStatistics	Gewährt die Erlaubnis, die Nutzungsstatistiken von Amazon GuardDuty in den letzten 30 Tagen für die angegebene Detektor-ID aufzulisten	Read			
InviteMembers	Gewährt die Berechtigung zum Einladen anderer AWS-Konten, GuardDuty zu aktivieren und zu GuardDuty-Mitgliedskonten zu werden.	Schreiben			
ListCoverage	Gewährt die Berechtigung zum Auflisten aller Ressourcendetails für ein bestimmtes Konto in einer Region	Auflisten	detector*		
ListDetectors	Gewährt die Berechtigung zum Abrufen einer Liste von GuardDuty-Detektoren.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListFilters	Gewährt die Berechtigung zum Abrufen einer Liste von GuardDuty-Filtern.	List			
ListFindings	Gewährt die Berechtigung zum Abrufen einer Liste von GuardDuty-Ergebnissen.	List			
ListIPSets	Gewährt die Berechtigung zum Abrufen einer Liste von GuardDuty-IPSets.	Auflisten			
ListInvitations	Gewährt die Berechtigung zum Abrufen einer Liste aller GuardDuty-Mitgliedschaftseinladungen, die an ein AWS-Konto gesendet wurden.	Auflisten			
ListMembers	Gewährt die Berechtigung zum Abrufen einer Liste von GuardDuty-Mitgliedskonten, die einem Administratorkonto zugeordnet sind.	Auflisten			
ListOrganizationAdminAccounts	Gewährt die Berechtigung, Details zum delegierten Organisationsadministrator für GuardDuty aufzulisten.	List			
ListPublishingDestinations	Gewährt die Berechtigung zum Abrufen einer Liste von Veröffentlichungszielen.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Abrufen einer Liste von Tags, die einer GuardDuty-Ressource zugeordnet sind.	Read	detector		
			filter		
			ipset		
			threatintelset		
ListThreatIntelSets	Gewährt die Berechtigung zum Abrufen einer Liste von GuardDuty ThreatIntelSets.	Auflisten			
SendSecurityTelemetry	Gewährt die Berechtigung zum Senden von Sicherheitstelemetriedaten für ein bestimmtes GuardDuty-Konto in einer Region	Schreiben			
StartMalwareScan	Gewährt die Berechtigung zum Initiieren eines neuen Malware-Scans	Schreiben			
StartMonitoringMembers	Gewährt einem GuardDuty-Administratorkonto die Berechtigung zum Überwachen der Ergebnisse von GuardDuty-Mitgliedskonten	Write			
StopMonitoringMembers	Gewährt die Berechtigung zum Deaktivieren von Überwachungsergebnissen von Mitgliedskonten.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer GuardDuty-Ressource.	Markieren	detector		
			filter		
			ipset		
			threatintelset		
				aws:RequestTag/${TagKey} aws:TagKeys	
UnarchiveFindings	Gewährt die Berechtigung zum Aufheben der Archivierung von GuardDuty-Ergebnissen.	Write			
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer GuardDuty-Ressource	Markieren	detector		
			filter		
			ipset		
			threatintelset		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateDetector	Gewährt die Berechtigung zum Aktualisieren von GuardDuty-Detektoren.	Write	detector*		
UpdateFilter	Gewährt die Berechtigung zum Aktualisieren von GuardDuty-Filtern.	Write	filter*		
UpdateFindingsFeedback	Gewährt die Berechtigung zum Aktualisieren des Ergebnis-Feedbacks, um GuardDuty-Ergebnisse als nützlich oder nicht nützlich zu kennzeichnen.	Write			
UpdateIPSet	Gewährt die Berechtigung zum Aktualisieren von GuardDuty-IPSets	Schreiben	ipset*		iam:DeleteRolePolicy iam:PutRolePolicy
UpdateMalwareScanSettings	Erteilung der Berechtigung zur Aktualisierung der Malware-Scaneinstellungen	Schreiben			
UpdateMemberDetectors	Gewährt die Berechtigung, zu aktualisieren, welche Datenquellen für Melder von Mitgliedskonten aktiviert sind	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateOrganizationConfiguration	Gewährt die Berechtigung zum Aktualisieren der Konfiguration des delegierten Administrators, der einem GuardDuty Detektor zugeordnet ist.	Write			
UpdatePublishingDestination	Gewährt die Berechtigung zum Aktualisieren eines Veröffentlichungsziels.	Write	publishingDestination*		s3:GetObject s3:ListBucket
UpdateThreatIntelSet	Gewährt die Berechtigung zum Aktualisieren der GuardDuty ThreatIntelSets.	Write	threatintelset*		iam:DeleteRolePolicy iam:PutRolePolicy

Von Amazon GuardDuty definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
detector	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}`	aws:ResourceTag/${TagKey}
filter	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/filter/${FilterName}`	aws:ResourceTag/${TagKey}
ipset	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/ipset/${IPSetId}`	aws:ResourceTag/${TagKey}
threatintelset	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/threatintelset/${ThreatIntelSetId}`	aws:ResourceTag/${TagKey}
publishingDestination	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/publishingDestination/${PublishingDestinationId}`	

Bedingungsschlüssel für Amazon GuardDuty

Amazon GuardDuty definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert Aktionen nach den Tag-Schlüsseln in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Health-APIs und -Benachrichtigungen

AWS Health APIs and Notifications (Servicepräfix: `health`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Health-APIs und -Benachrichtigungen definierte Aktionen
- Von AWS Health-APIs and -Benachrichtigungen definierte Ressourcentypen
- Bedingungsschlüssel für AWS Health-APIs und -Benachrichtigungen

Von AWS Health-APIs und -Benachrichtigungen definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeAffectedAccountsForOrganization	Gewährt die Berechtigung zum Abrufen einer Liste von Konten, die von den angegebenen Ereignissen in der Organisation betroffen sind	Lesen			organizations:ListAccounts
DescribeAffectedEntities	Gewährt die Berechtigung zum Abrufen einer Liste von Entitäten, die von den angegebenen Ereignissen betroffen sind	Lesen	event*		
				health:eventTypeCode health:service	
DescribeAffectedEntitiesForOrganization	Gewährt die Berechtigung zum Abrufen einer Liste von Entitäten, die von den angegebenen Ereignissen und Konten in der Organisation betroffen sind	Lesen			organizations:ListAccounts
DescribeEntityAggregates	Gewährt die Berechtigung zum Zurückgeben der Anzahl von Entitäten, die von jedem der angegebenen Ereignisse betroffen sind	Lesen			
DescribeEntityAggregatesForOrganization	Gewährt die Berechtigung zum Zurückgeben der Anzahl von Entitäten, die von jedem der angegebenen Ereignisse	Lesen			organizations:ListAccounts

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	in einer Organisation betroffen sind				
DescribeEventAggregates	Gewährt die Berechtigung zum Abrufen der Anzahl von Ereignissen jedes Ereignistyps (Problem, geplante Änderung und Kontobenachrichtigung)	Lesen			
DescribeEventDetails	Gewährt die Berechtigung zum Abrufen detaillierter Informationen zu einem oder mehreren angegebenen Ereignissen	Lesen	event*		
				health:eventTypeCode health:service	
DescribeEventDetailsForOrganization	Gewährt die Berechtigung zum Abrufen detaillierter Informationen zu einem oder mehreren angegebenen Ereignissen für angegebene Konten in der Organisation	Lesen			organizations:ListAccounts
DescribeEventTypes	Gewährt die Berechtigung zum Abrufen der Ereignistypen, die den angegebenen Filterkriterien entsprechen	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeEvents	Gewährt die Berechtigung zum Abrufen von Informationen zu Ereignissen, die den angegebenen Filterkriterien entsprechen	Lesen			
DescribeEventsForOrganization	Gewährt die Berechtigung zum Abrufen von Informationen zu Ereignissen, die den angegebenen Filterkriterien in einer Organisation entsprechen	Lesen			organizations:ListAccounts
DescribeHealthServiceStatusForOrganization	Gewährt die Berechtigung zum Abrufen des Status der Aktivierung oder Deaktivierung des Features „Organisationsansicht“	Lesen			organizations:ListAccounts
DisableHealthServiceAccessForOrganization	Gewährt die Berechtigung zum Deaktivieren des Features „Organisationsansicht“	Berechtigungsverwaltung			organizations:DisableAWSServiceAccess organizations:ListAccounts

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
EnableHealthServiceAccessForOrganization	Gewährt die Berechtigung zum Aktivieren des Features „Organisationsansicht“	Berechtigungsverwaltung			iam:CreateServiceLinkedRole organizations:EnableAWSServiceAccess organizations:ListAccounts

Von AWS Health-APIs and -Benachrichtigungen definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
event	`arn:${Partition}:health:*::event/${Service}/${EventTypeCode}/*`	

Bedingungsschlüssel für AWS Health-APIs und -Benachrichtigungen

AWS Health APIs and Notifications definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
health:eventTypeCode	Filtert den Zugriff nach Ereignistyp	Zeichenfolge
health:service	Filtert den Zugriff nach betroffenem Service	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für AWS HealthImaging

AWS HealthImaging (Service-Präfix: `medical-imaging`) bietet die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS HealthImaging definierte Aktionen
- Von AWS HealthImaging definierte Ressourcentypen
- Zustandsschlüssel für AWS HealthImaging

Von AWS HealthImaging definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CopyImageSet	Gewährt die Berechtigung zum Kopieren eines Imagesatzes	Schreiben	datastore*		
			imageset*		
CreateDatastore	Gewährt die Berechtigung zum Erstellen eines Datenspeichers für die Aufnahme von Bilddaten	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDatastore	Gewährt die Berechtigung zum Löschen eines Datenspeichers	Schreiben	datastore*		
DeleteImageSet	Gewährt die Berechtigung zum Löschen eines Imagesatzes	Schreiben	datastore*		
			imageset*		
GetDICOMImportJob	Gewährt die Berechtigung zum Abrufen der Eigenschaften eines Importauftrags	Lesen	datastore*		
GetDatastore	Gewährt die Berechtigung zum Abrufen von Datenspeichereigenschaften	Lesen	datastore*		
GetImageFrame	Gewährt die Berechtigung zum Abrufen von Imageframeeigenschaften	Lesen	datastore*		
			imageset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetImageSet	Gewährt die Berechtigung zum Abrufen von Imagesatz eigenschaften	Lesen	datastore*		
			imageset*		
GetImageSetMetadata	Gewährt die Berechtigung zum Abrufen von Imagesatz metadateneigenschaften	Lesen	datastore*		
			imageset*		
ListDICOMImportJobs	Gewährt die Berechtigung zum Abrufen einer Liste von Importaufträgen für einen Datenspeicher	Auflisten	datastore*		
ListDatastores	Gewährt die Berechtigung zum Auflisten von Datenspeichern	Auflisten			
ListImageSetVersions	Gewährt die Berechtigung zum Auflisten der Versionen eines Imagesatzes	Auflisten	datastore*		
			imageset*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource für medizinische Bildgebung	Auflisten	datastore		
			imageset		
SearchImageSets	Gewährt die Berechtigung zum Suchen nach Imagesätzen	Lesen	datastore*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartDICOMImportJob	Gewährt die Berechtigung zum Starten eines DICOM-Importauftrags	Schreiben	datastore*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Ressource für medizinische Bildgebung	Markierung	datastore		
			imageset		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags von einer Ressource für medizinische Bildgebung	Markierung	datastore		
			imageset		
				aws:TagKeys	
UpdateImageSetMetadata	Gewährt die Berechtigung zum Aktualisieren von Imagesatzmetadaten eigenschaften	Schreiben	datastore*		
			imageset*		

Von AWS HealthImaging definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
datastore	`arn:${Partition}:medical-imaging:${Region}:${Account}:datastore/${DatastoreId}`	aws:ResourceTag/${TagKey}
imageset	`arn:${Partition}:medical-imaging:${Region}:${Account}:datastore/${DatastoreId}/imageset/${ImageSetId}`	aws:ResourceTag/${TagKey}

Zustandsschlüssel für AWS HealthImaging

AWS HealthImaging definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wertepaaren, die in der Anforderung zulässig sind	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paar einer Ressource	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach Liste von Tag-Schlüsseln, die in der Anforderung zulässig sind	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS HealthLake

AWS HealthLake (Dienstpräfix:`healthlake`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS HealthLake definierte Aktionen
- Von AWS HealthLake definierte Ressourcentypen
- Bedingungsschlüssel für AWS HealthLake

Von AWS HealthLake definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateFHIRDatastore	Gewährt die Berechtigung zum Erstellen eines Datenspeichers, der FHIR-Daten aufnehmen und exportieren kann	Write		aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
CreateResource	Gewährt die Berechtigung zum Erstellen von Ressourcen	Write	datastore*		
DeleteFHIRDatastore	Gewährt die Berechtigung zum Löschen eines Datenspeichers	Write	datastore*		
DeleteResource	Gewährt die Berechtigung zum Löschen von Ressourcen	Write	datastore*		
DescribeFHIRDatastore	Gewährt die Berechtigung zum Abrufen der mit dem FHIR-Datenspeicher verbundenen Eigenschaften, einschließlich der Datenspeicher-ID, des Datenspeicher-ARN, des Datenspeichernamens, des Datenspeicherstatus, erstellt bei, Version des Datenspeicher-Typs und Datenspeicher-Endpunkts	Read	datastore*		
DescribeFHIRExportJob	Gewährt die Berechtigung, die Eigenschaften eines FHIR-Exportauftrags anzuzeigen, einschließlich ID, ARN, Name und Status des Datenspeichers	Read	datastore*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeFHIRImportJob	Gewährt die Berechtigung zum Anzeigen der Eigenschaften eines FHIR-Importauftrags, einschließlich ID, ARN, Name und Status des Datenspeichers	Read	datastore*		
GetCapabilities	Gewährt die Berechtigung zum Abrufen der Funktionen eines FHIR-Datenspeichers	Read	datastore*		
ListFHIRDatastores	Gewährt die Berechtigung, alle FHIR-Datenspeicher aufzulisten, die sich im Konto des Benutzers befinden, unabhängig vom Datenspeicherstatus	List			
ListFHIRExportJobs	Gewährt die Berechtigung zum Abrufen einer Liste von Exportaufträgen für den angegebenen Datenspeicher	List	datastore*		
ListFHIRImportJobs	Gewährt die Berechtigung zum Abrufen einer Liste von Importaufträgen für den angegebenen Datenspeicher	List	datastore*		
ListTagsForResource	Gewährt die Berechtigung zum Abrufen von Tags für die angegebene Ressource	Read	datastore		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ReadResource	Gewährt die Berechtigung zum Lesen von Ressourcen	Lesen	datastore*		
SearchEverything	Erteilt die Erlaubnis, alle Ressourcen zu durchsuchen, die sich auf einen Patienten beziehen	Lesen	datastore*		
SearchWithGet	Gewährt die Berechtigung, Ressourcen mit der GET-Methode zu durchsuchen	Read	datastore*		
SearchWithPost	Gewährt die Berechtigung, Ressourcen mit der POST-Methode zu durchsuchen	Read	datastore*		
StartFHIRExportJob	Gewährt die Berechtigung, eine FHIR-Export-Aufgabe zu beginnen	Write	datastore*		
StartFHIRImportJob	Gewährt die Berechtigung, eine FHIR-Import-Aufgabe zu beginnen	Write	datastore*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einem Datenspeicher.	Markieren	datastore		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags, die einem Datenspeicher zugeordnet sind.	Markieren	datastore		
				aws:TagKeys	
UpdateResource	Gewährt die Berechtigung zum Aktualisieren von Ressourcen	Schreiben	datastore*		

Von AWS HealthLake definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
datastore	`arn:${Partition}:healthlake:${Region}:${Account}:datastore/fhir/${DatastoreId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS HealthLake

AWS HealthLake definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüsselwertpaaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS HealthOmics

AWS HealthOmics (Servicepräfix: `omics`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS HealthOmics definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AbortMultipartReadSetUpload	Gewährt die Berechtigung zum Abbrechen von Read-Set-Uploads	Schreiben	sequenceStore*		
AcceptShare	Gewährt die Berechtigung zum Annehmen einer Freigabe	Schreiben			
BatchDeleteReadSet	Gewährt die Berechtigung zum Löschen von Lesesätzen im angegebenen Sequence Store	Schreiben	sequenceStore*		
CancelAnnotationImportJob	Gewährt die Berechtigung zum Abbrechen eines Annotations-Importauftrags	Schreiben	AnnotationImportJob*		
CancelRun	Gewährt die Berechtigung zum Abbrechen einer Workflow-Ausführung und zum Abbrechen von allen Workflow-Aufgaben	Schreiben	run*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelVariantImportJob	Gewährt die Berechtigung zum Abbrechen eines Variations-Importauftrags	Schreiben	VariantImportJob*		
CompleteMultipartReadSetUpload	Gewährt die Berechtigung zum Abschließen eines Read-Set-Uploads	Schreiben	sequenceStore*		
CreateAnnotationStore	Gewährt die Berechtigung zum Erstellen eines Annotationsspeichers	Schreiben			
CreateAnnotationStoreVersion	Gewährt die Berechtigung zum Erstellen einer Version in einem Annotationsspeicher	Schreiben	AnnotationStore*		
CreateMultipartReadSetUpload	Gewährt die Berechtigung zum Erstellen eines Read-Set-Uploads	Schreiben	sequenceStore*		
CreateReferenceStore	Gewährt die Berechtigung zum Erstellen eines Reference Stores	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRunGroup	Gewährt die Berechtigung zum Erstellen einer neuen Workflow-Ausführungsgruppe	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSequenceStore	Gewährt die Berechtigung zum Erstellen eines Sequence Stores	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateShare	Gewährt die Berechtigung zum Erstellen einer Freigabe	Schreiben			
CreateVariantStore	Gewährt die Berechtigung zum Erstellen eines Variant Stores	Schreiben			
CreateWorkflow	Gewährt die Berechtigung, einen neuen Workflow mit einer Workflow-Definition und einer Vorlage von Workflow-Parametern zu erstellen	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAnnotationStore	Gewährt die Berechtigung zum Löschen eines Annotationsspeichers	Schreiben	AnnotationStore*		
DeleteAnnotationStoreVersions	Gewährt die Berechtigung zum Löschen von Versionen in einem Annotationsspeicher	Schreiben	AnnotationStore* AnnotationStoreVersion*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteReference	Gewährt die Berechtigung zum Löschen einer Referenz im angegebenen Referenzspeicher	Schreiben	reference*		
			referenceStore*		
DeleteReferenceStore	Gewährt die Berechtigung zum Löschen eines Reference Stores	Schreiben	referenceStore*		
DeleteRun	Gewährt die Berechtigung zum Löschen einer Workflowausführung	Schreiben	run*		
DeleteRunGroup	Gewährt die Berechtigung zum Löschen einer Workflowausführungsgruppe	Schreiben	runGroup*		
DeleteSequenceStore	Gewährt die Berechtigung zum Löschen eines Sequence Stores	Schreiben	sequenceStore*		
DeleteShare	Gewährt die Berechtigung zum Löschen einer Freigabe	Schreiben			
DeleteVariantStore	Gewährt die Berechtigung zum Löschen eines Variant Stores	Schreiben	VariantStore*		
DeleteWorkflow	Gewährt die Berechtigung zum Löschen eines Workflows	Schreiben	workflow*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAnnotationImportJob	Gewährt die Berechtigung zum Abrufen des Status eines Annotations-Importauftrags	Lesen	AnnotationImportJob*		
GetAnnotationStore	Gewährt die Berechtigung zum Abrufen detaillierter Informationen zu einem Annotationsspeicher	Lesen	AnnotationStore*		
GetAnnotationStoreVersion	Gewährt die Berechtigung zum Abrufen detaillierter Informationen über eine Version in einem Annotationsspeicher	Lesen	AnnotationStore*		
			AnnotationStoreVersion*		
GetReadSet	Gewährt die Berechtigung zum Abrufen eines Lesesatzes im angegebenen Sequenzspeicher	Lesen	readSet*		
			sequenceStore*		
GetReadSetActivationJob	Gewährt die Berechtigung zum Abrufen von Details zu einem Lesesatz-Aktivierungsauftrag für den angegebenen Sequence Store	Lesen	sequenceStore*		
GetReadSetExportJob	Gewährt die Berechtigung zum Abrufen von Details zu einem Lesesatz-Exportauftrag für den angegebenen Sequence Store	Lesen	sequenceStore*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetReadSetImportJob	Gewährt die Berechtigung zum Abrufen von Details zu einem Lesesatz-Importauftrag für den angegebenen Sequence Store	Lesen	sequenceStore*		
GetReadSetMetadata	Gewährt die Berechtigung zum Abrufen von Details zu einem Lesesatz für den angegebenen Sequence Store	Lesen	readSet*		
			sequenceStore*		
GetReference	Gewährt die Berechtigung zum Abrufen einer Referenz im angegebenen Reference Store	Lesen	reference*		
			referenceStore*		
GetReferenceImportJob	Gewährt die Berechtigung zum Abrufen von Details zu einer Referenz-Importaufgabe für den angegebenen Reference Store	Lesen	referenceStore*		
GetReferenceMetadata	Gewährt die Berechtigung zum Abrufen von Details zu einer Referenz im angegebenen Referenzspeicher	Lesen	reference*		
			referenceStore*		
GetReferenceStore	Gewährt die Berechtigung zum Abrufen von Details zu einem Referenzspeicher	Lesen	referenceStore*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetRun	Gewährt die Berechtigung zum Abrufen eines Workflowausführungsdetails	Lesen	run*		
GetRunGroup	Gewährt die Berechtigung zum Abrufen eines Workflowausführungsgruppendetails	Lesen	runGroup*		
GetRunTask	Gewährt die Berechtigung zum Abrufen eines Workflowsaufgabendetails	Lesen	TaskResource*		
			run*		
GetSequenceStore	Gewährt die Berechtigung zum Abrufen von Details zu einem Sequenzspeicher	Lesen	sequenceStore*		
GetShare	Gewährt die Berechtigung zum Abrufen detaillierter Informationen über eine Freigabe	Lesen			
GetVariantImportJob	Gewährt die Berechtigung zum Abrufen des Status eines Variantenimportauftrags	Lesen	VariantImportJob*		
GetVariantStore	Gewährt die Berechtigung zum Abrufen detaillierter Informationen zu einem Variationsspeicher	Lesen	VariantStore*		
GetWorkflow	Gewährt die Berechtigung zum Abrufen eines Workflowsdetails	Lesen	workflow*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAnnotationImportJobs	Gewährt die Berechtigung zum Abrufen einer Liste von Annotations-Importaufträgen	Auflisten			
ListAnnotationStoreVersions	Gewährt die Berechtigung zum Abrufen einer Liste von Informationen über Versionen in einem Annotationsspeicher	Auflisten	AnnotationStore*		
ListAnnotationStores	Gewährt die Berechtigung zum Abrufen einer Liste von Informationen zu Annotation Stores	Auflisten			
ListMultipartReadSetUploads	Gewährt die Berechtigung zum Auflisten von Read-Set-Uploads	Auflisten	sequenceStore*		
ListReadSetActivationJobs	Gewährt die Berechtigung zum Auflisten von Lesesatz-Aktivierungsaufträgen für den angegebenen Sequenzspeicher	Auflisten	sequenceStore*		
ListReadSetExportJobs	Gewährt die Berechtigung zum Auflisten von Lesesatz-Exportaufträgen für den angegebenen Sequence Store	Auflisten	sequenceStore*		
ListReadSetImportJobs	Gewährt die Berechtigung zum Auflisten von Lesesatz-Importaufträgen für den angegebenen Sequence Store	Auflisten	sequenceStore*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListReadSetUploadParts	Gewährt die Berechtigung zur Auflistung von Read-Set-Uploadteilen	Auflisten	sequenceStore*		
ListReadSets	Gewährt die Berechtigung zum Auflisten von Lesesätzen im angegebenen Sequence Store	Auflisten	sequenceStore*		
ListReferenceImportJobs	Gewährt die Berechtigung zum Auflisten von Referenz-Importaufträgen für den angegebenen Reference Store	Auflisten	referenceStore*		
ListReferenceStores	Gewährt die Berechtigung zum Auflisten von Referenzspeichers	Auflisten			
ListReferences	Gewährt die Berechtigung zum Auflisten von Referenzen im angegebenen Referenzspeicher	Auflisten	referenceStore*		
ListRunGroups	Gewährt die Berechtigung zum Abrufen einer Liste aller Ausführungsgruppen eines Workflows	Auflisten			
ListRunTasks	Gewährt die Berechtigung zum Abrufen einer Liste von Aufgaben aller Ausführungen eines Workflows	Auflisten	run*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListRuns	Gewährt die Berechtigung zum Abrufen einer Liste aller Ausführungen eines Workflows	Auflisten			
ListSequenceStores	Gewährt die Berechtigung zum Auflisten von Sequenzspeichern	Auflisten			
ListShares	Gewährt die Berechtigung zum Abrufen einer Liste von Informationen über Freigaben	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Abrufen einer Liste von Ressourcen-AWS-Tags	Auflisten			
ListVariantImportJobs	Gewährt die Berechtigung zum Abrufen einer Liste von Varianten-Importaufträgen	Auflisten			
ListVariantStores	Gewährt die Berechtigung zum Abrufen einer Liste von Metadaten, die für den Variantenspeicher gespeichert sind	Auflisten			
ListWorkflows	Gewährt die Berechtigung zum Abrufen einer Liste von verfügbaren Workflows	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartAnnotationImportJob	Gewährt die Berechtigung zum Importieren einer Liste von Annotationsdateien in einen Annotation Store	Schreiben			
StartReadSetActivationJob	Gewährt die Berechtigung zum Starten eines Lesesatz-Aktivierungsauftrags aus dem angegebenen Sequence Store	Schreiben	sequenceStore*		
StartReadSetExportJob	Gewährt die Berechtigung zum Starten eines Lesesatz-Exportauftrags aus dem angegebenen Sequence Store	Schreiben	sequenceStore*		
StartReadSetImportJob	Gewährt die Berechtigung zum Starten eines Lesesatz-Importauftrags in den angegebenen Sequence Store	Schreiben	sequenceStore*		
StartReferenceImportJob	Gewährt die Berechtigung zum Starten eines Referenz-Importauftrags in den angegebenen Reference Store	Schreiben	referenceStore*		
StartRun	Gewährt die Berechtigung zum Starten eines Workflows	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartVariantImportJob	Gewährt die Berechtigung zum Importieren einer Liste von Variantendateien in einen Variant Store	Schreiben			
TagResource	Gewährt die Berechtigung zum Hinzufügen von AWS Tags zu einer Ressource	Markierung	readSet		
			reference		
			referenceStore		
			run		
			runGroup		
			sequenceStore		
			workflow		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Ressourcentags AWS	Markierung	readSet		
			reference		
			referenceStore		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			run		
			runGroup		
			sequenceStore		
			workflow		
				aws:TagKeys	
UpdateAnnotationStore	Gewährt die Berechtigung zum Aktualisieren von Informationen zum Annotationsspeicher	Schreiben	AnnotationStore*		
UpdateAnnotationStoreVersion	Gewährt die Berechtigung zum Aktualisieren der Informationen über die Version in einem Annotationsspeicher	Schreiben	AnnotationStore*		
			AnnotationStoreVersion*		
UpdateRunGroup	Gewährt die Berechtigung zum Aktualisieren einer Workflow-Ausführungsgruppe	Schreiben	runGroup*		
UpdateVariantStore	Gewährt die Berechtigung zum Aktualisieren der Metadaten über den Variantenspeicher	Schreiben	VariantStore*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateWorkflow	Gewährt die Berechtigung zum Aktualisieren von Workflowsdetails	Schreiben	workflow*		
UploadReadSetPart	Gewährt die Berechtigung zum Hochladen von Read-Set-Teilen	Schreiben	sequenceStore*		

Von AWS HealthOmics definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
AnnotationImportJob	`arn:${Partition}:omics:${Region}:${Account}:annotationImportJob/${AnnotationImportJobId}`	omics:AnnotationImportJobJobId
AnnotationStore	`arn:${Partition}:omics:${Region}:${Account}:annotationStore/${AnnotationStoreId}`	omics:AnnotationStoreName
AnnotationStoreVersion	`arn:${Partition}:omics:${Region}:${Account}:annotationStore/${AnnotationStoreName}/version/${AnnotationStoreVersionName}`	omics:AnnotationStoreVersionName

Ressourcentypen	ARN	Bedingungsschlüssel
readSet	arn:${Partition}:omics:${Region}:${Account}:sequenceStore/${SequenceStoreId}/readSet/${ReadSetId}	aws:ResourceTag/${TagKey}
reference	arn:${Partition}:omics:${Region}:${Account}:referenceStore/${ReferenceStoreId}/reference/${ReferenceId}	aws:ResourceTag/${TagKey}
referenceStore	arn:${Partition}:omics:${Region}:${Account}:referenceStore/${ReferenceStoreId}	aws:ResourceTag/${TagKey}
run	arn:${Partition}:omics:${Region}:${Account}:run/${Id}	aws:ResourceTag/${TagKey}
runGroup	arn:${Partition}:omics:${Region}:${Account}:runGroup/${Id}	aws:ResourceTag/${TagKey}
sequenceStore	arn:${Partition}:omics:${Region}:${Account}:sequenceStore/${SequenceStoreId}	aws:ResourceTag/${TagKey}
TaggingResource	arn:${Partition}:omics:${Region}:${Account}:tag/${TagKey}	
TaskResource	arn:${Partition}:omics:${Region}:${Account}:task/${Id}	
VariantImportJob	arn:${Partition}:omics:${Region}:${Account}:variantImportJob/${VariantImportJobId}	omics:VariantImportJobJobId
VariantStore	arn:${Partition}:omics:${Region}:${Account}:variantStore/${VariantStoreId}	omics:VariantStoreName

Ressourcentypen	ARN	Bedingungsschlüssel
workflow	`arn:${Partition}:omics:${Region}:${Account}:workflow/${Id}`	aws:ResourceTag/${TagKey}

Zustandsschlüssel für AWS HealthOmics

AWS HealthOmics definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüsselwertpaaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString
omics:AnnotationImportJobJobId	Filtert den Zugriff nach einer eindeutigen Ressourcenkennung	Zeichenfolge
omics:AnnotationStoreName	Filtert den Zugriff nach dem Namen des Speichers	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
omics:AnnotationStoreVersionName	Filtert den Zugriff nach dem Namen der Version des Annotationsspeichers	Zeichenfolge
omics:VariantImportJobJobId	Filtert den Zugriff nach einer eindeutigen Ressourcenkennung	Zeichenfolge
omics:VariantStoreName	Filtert den Zugriff nach dem Namen des Speichers	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für ausgehende Kommunikation mit hohem Volumen

Ausgehende Kommunikation mit hohem Volumen (Service-Präfix: `connect-campaigns`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Aktionen, die durch ausgehende Kommunikation mit hohem Volumen definiert werden
- Ressourcentypen definiert durch ausgehende Kommunikation mit hohem Volumen
- Bedingungsschlüssel für ausgehende Kommunikation mit hohem Volumen

Aktionen, die durch ausgehende Kommunikation mit hohem Volumen definiert werden

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCampaign	Gewährt die Berechtigung zum Erstellen einer Kampagne	Schreiben	campaign*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteCampaign	Gewährt die Berechtigung zum Löschen einer Kampagne	Schreiben	campaign*		
DeleteConnectInstanceConfig	Gewährt die Berechtigung zum Entfernen von Konfigurationsinformationen für eine Amazon-Connect-Instance	Schreiben			
DeleteInstanceOnboardingJob	Gewährt die Berechtigung zum Entfernen des Onboarding-Jobs für eine Amazon-Connect-Instance	Schreiben			
DescribeCampaign	Gewährt die Berechtigung zum Beschreiben einer bestimmten Kampagne	Lesen	campaign*		
				aws:RequestTag/${TagKey}	
GetCampaignState	Gewährt die Berechtigung zum Abrufen des Status einer Kampagne	Lesen	campaign*		
				aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetCampaignStateBatch	Gewährt die Berechtigung zum Abrufen des Status von Kampagnen	Lesen	campaign*		
				aws:RequestTag/${TagKey}	
GetConnectInstanceConfig	Gewährt die Berechtigung zum Abrufen von Konfigurationsinformationen für eine Amazon-Connect-Instance	Lesen			
GetInstanceOnboardingJobStatus	Gewährt die Berechtigung zum Abrufen des Onboarding-Auftragsstatus für eine Amazon-Connect-Instance	Lesen			
ListCampaigns	Gewährt die Berechtigung zum Abrufen einer Zusammenfassung aller Kampagnen	Auflisten		aws:RequestTag/${TagKey}	
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen	campaign		
				aws:ResourceTag/${TagKey}	
PauseCampaign	Gewährt die Berechtigung zum Pausieren einer Kampagne	Schreiben	campaign*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutDialRequestBatch	Gewährt die Berechtigung zum Erstellen von Wählanforderungen für die angegebene Kampagne	Schreiben	campaign*		
ResumeCampaign	Gewährt die Berechtigung zur Fortsetzung einer Kampagne	Schreiben	campaign*		
StartCampaign	Gewährt die Berechtigung zum Beginnen einer Kampagne	Schreiben	campaign*		
StartInstanceOnboardingJob	Gewährt die Berechtigung zum Starten des Onboarding-Jobs für eine Amazon-Connect-Instance	Schreiben			
StopCampaign	Gewährt die Berechtigung zum Stoppen einer Kampagne	Schreiben	campaign*		
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren	campaign		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Markierung	campaign		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateCampaignDialerConfig	Gewährt die Berechtigung zum Aktualisieren der Wähler-Konfiguration einer Kampagne	Schreiben	campaign*		
UpdateCampaignName	Gewährt die Berechtigung, den Namen einer Kampagne zu aktualisieren	Schreiben	campaign*		
UpdateCampaignOutboundCallConfig	Gewährt die Berechtigung zum Aktualisieren der Konfiguration für ausgehende Anrufe einer Kampagne	Schreiben	campaign*		

Ressourcentypen definiert durch ausgehende Kommunikation mit hohem Volumen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
campaign	`arn:${Partition}:connect-campaigns:${Region}:${Account}:campaign/${CampaignId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für ausgehende Kommunikation mit hohem Volumen

Die ausgehende Kommunikation mit hohem Volumen definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung.	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf den Tag-Schlüssel-Wert-Paaren, die an die Ressource angefügt wurden.	Zeichenfolge
aws:TagKeys	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Honeycode

Amazon Honeycode (Servicepräfix: `honeycode`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Honeycode definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ApproveTeamAssociation [nur Berechtigung]	Gewährt die Berechtigung zum Genehmigen einer Teammappingsanfrage für Ihr AWS-Konto	Write			
BatchCreateTableRows	Gewährt die Berechtigung zum Erstellen neuer Zeilen in einer Tabelle	Write	table*		
BatchDeleteTableRows	Gewährt die Berechtigung zum Löschen von Zeilen aus einer Tabelle	Write	table*		
BatchUpdateTableRows	Gewährt die Berechtigung zum Aktualisieren von Zeilen in einer Tabelle	Write	table*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchUpsertTableRows	Gewährt die Berechtigung zum Upsert von Zeilen in einer Tabelle	Write	table*		
CreateTeam [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines neuen Amazon-Honeycode-Teams für Ihr AWS-Konto	Write			
CreateTenant [nur Berechtigung]	Gewährt die Berechtigung, in Amazon Honeycode einen neuen Mandanten für Ihr AWS-Konto zu erstellen	Write			
DeleteDomains [nur Berechtigung]	Gewährt die Berechtigung zum Löschen von Amazon-Honeycode-Domains für Ihr AWS-Konto	Schreiben			
DeregisterGroups [nur Berechtigung]	Gewährt die Berechtigung zum Entfernen von Gruppen aus einem Amazon-Honeycode-Team für Ihr AWS-Konto	Write			
DescribeTableDataImportJob	Gewährt die Berechtigung zum Abrufen von Details zu einer Tabellendaten-Importaufgabe	Read	table*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeTeam [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Details über Amazon-Honeycode-Teams für Ihr AWS-Konto	Read			
GetScreenData	Gewährt die Berechtigung zum Laden der Daten von einem Bildschirm	Read	screen*		
InvokeScreenAutomation	Gewährt die Berechtigung zum Aufrufen einer Bildschirmautomatisierung	Write	screen-automation*		
ListDomains [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aller Amazon-Honeycode-Domains und ihrer Verifizierungsstatus für Ihr AWS-Konto	List			
ListGroups [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aller Gruppen in einem Amazon-Honeycode-Team für Ihr AWS-Konto	List			
ListTableColumns	Gewährt die Berechtigung zum Auflisten der Spalten in einer Tabelle	List	table*		
ListTableRows	Gewährt die Berechtigung zum Auflisten der Zeilen in einer Tabelle	List	table*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTables	Gewährt die Berechtigung zum Auflisten der Tabellen in einer Arbeitsmappe	Auflisten	workbook*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten aller Tags für eine Ressource	Markierung			
ListTeamAssociations [nur Berechtigung]	Gewährt die Berechtigung, alle ausstehenden und genehmigten Teammappingen mit Ihrem AWS-Konto aufzulisten	List			
ListTenants [nur Berechtigung]	Gewährt die Berechtigung, alle Mandanten von Amazon Honeycode für Ihr AWS-Konto aufzulisten	List			
QueryTableRows	Gewährt die Berechtigung, die Zeilen einer Tabelle mit einem Filter abzufragen	Read	table*		
RegisterDomainForVerification [nur Berechtigung]	Gewährt die Berechtigung zum Anfordern einer Überprüfung der Amazon-Honeycode-Domains für Ihr AWS-Konto	Write			
RegisterGroups [nur Berechtigung]	Gewährt die Berechtigung zum Hinzufügen von Gruppen zu einem Amazon-Honeycode-Team für Ihr AWS-Konto	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RejectTeamAssociation [nur Berechtigung]	Gewährt die Berechtigung zum Ablehnen einer Teammappingsanfrage für Ihr AWS-Konto	Write			
RestartDomainVerification [nur Berechtigung]	Gewährt die Berechtigung zum Neustarten der Überprüfung der Amazon-Honeycode-Domains für Ihr AWS-Konto	Write			
StartTableDataImportJob	Gewährt die Berechtigung zum Starten einer Tabellendaten-Importaufgabe	Schreiben	table*		
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren			
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Markieren			
UpdateTeam [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren eines Amazon-Honeycode-Teams für Ihr AWS-Konto	Write			

Von Amazon Honeycode definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
workbook	`arn:${Partition}:honeycode:${Region}:${Account}:workbook:workbook/${WorkbookId}`	
table	`arn:${Partition}:honeycode:${Region}:${Account}:table:workbook/${WorkbookId}/table/${TableId}`	
screen	`arn:${Partition}:honeycode:${Region}:${Account}:screen:workbook/${WorkbookId}/app/${AppId}/screen/${ScreenId}`	
screen-automation	`arn:${Partition}:honeycode:${Region}:${Account}:screen-automation:workbook/${WorkbookId}/app/${AppId}/screen/${ScreenId}/automation/${AutomationId}`	

Bedingungsschlüssel für Amazon Honeycode

Honeycode besitzt keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS IAM Access Analyzer

AWS IAM Access Analyzer (Service-Präfix: `access-analyzer`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien zur Verfügung.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS IAM Access Analyzer definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ApplyArchiveRule	Gewährt die Berechtigung zum Anwenden einer Archivierungsregel	Write	Analyzer*		
CancelPolicyGeneration	Gewährt die Berechtigung zum Abbrechen einer Richtliniengenerierung	Schreiben			
CheckAccessNotGranted	Gewährt die Berechtigung, zu überprüfen, ob der angegebene Zugriff aufgrund einer Richtlinie nicht zulässig ist	Lesen			
CheckNoNewAccess	Gewährt die Berechtigung, zu überprüfen, ob im Vergleich zu einer vorhandenen Richtlinie kein neuer Zugriff zulässig ist	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAccessPreview	Gewährt die Berechtigung zum Erstellen einer Zugriffsvorschau für den angegebenen Analyzer	Write	Analyzer*		
CreateAnalyzer	Gewährt die Berechtigung zum Erstellen eines Analyzers	Write	Analyzer*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateArchiveRule	Gewährt die Berechtigung zum Erstellen einer Archivierungsregel für den angegebenen Analyzer	Write	ArchiveRule*		
DeleteAnalyzer	Gewährt die Berechtigung zum Löschen des angegebenen Analyzers	Write	Analyzer*		
DeleteArchiveRule	Gewährt die Berechtigung zum Löschen von Archivierungsregeln für den angegebenen Analyzer	Write	ArchiveRule*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAccessPreview	Gewährt die Berechtigung zum Abrufen von Informationen über eine Zugriffsvorschau	Read	Analyzer*		
GetAnalyzedResource	Gewährt die Berechtigung zum Abrufen von Informationen über eine analysierte Ressource	Read	Analyzer*		
GetAnalyzer	Gewährt die Berechtigung zum Abrufen von Informationen über Analyzer	Read	Analyzer*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetArchiveRule	Gewährt die Berechtigung zum Abrufen von Informationen über Archivierungsregeln für den angegebenen Analyzer	Read	ArchiveRule*		
GetFinding	Gewährt die Berechtigung zum Abrufen von Ergebnissen	Lesen	Analyzer*		
GetFindingsStatistics [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Statistiken zu Ergebnissen	Lesen	Analyzer*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetGeneratedPolicy	Gewährt die Berechtigung zum Abrufen einer Richtlinie, die mit StartPolicyGeneration generiert wurde	Read			
ListAccessPreviewFindings	Gewährt die Berechtigung zum Abrufen einer Liste von Ergebnissen aus einer Zugriffsvorschau	Read	Analyzer*		
ListAccessPreviews	Gewährt die Berechtigung zum Abrufen einer Liste von Zugriffsvorschauen	List	Analyzer*		
ListAnalyzedResources	Gewährt die Berechtigung zum Abrufen einer Liste von analysierten Ressourcen	Read	Analyzer*		
ListAnalyzers	Gewährt die Berechtigung zum Abrufen einer Liste von Analyzern	List			
ListArchiveRules	Gewährt die Berechtigung zum Abrufen einer Liste von Archivierungsregeln von einem Analyzer	List	Analyzer*		
ListFindings	Gewährt die Berechtigung zum Abrufen einer Liste von Ergebnissen aus einem Analyzer	Read	Analyzer*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListPolicyGenerations	Gewährt die Berechtigung zum Auflisten aller kürzlich gestarteten Richtliniengenerierungen	Read			
ListTagsForResource	Gewährt die Berechtigung zum Abrufen einer Liste von Tags, die auf eine Ressource angewendet wurden	Read	Analyzer		
StartPolicyGeneration	Gewährt die Berechtigung zum Starten einer Richtliniengenerierung	Write			iam:PassRole
StartResourceScan	Gewährt die Berechtigung zum Starten eines Scans der auf eine Ressource angewandten Richtlinien	Write	Analyzer*		
TagResource	Gewährt die Berechtigung zum Hinzufügen eines Tags zu einer Ressource	Markieren	Analyzer		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen eines Tags von einer Ressource	Markieren	Analyzer		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateArchiveRule	Gewährt die Berechtigung zum Ändern einer Archivierungsregel	Write	ArchiveRule*		
UpdateFindings	Gewährt die Berechtigung zum Ändern von Ergebnissen	Write	Analyzer*		
ValidatePolicy	Gewährt die Berechtigung zurm Validieren einer Richtlinie	Read			

Von AWS IAM Access Analyzer definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Analyzer	`arn:${Partition}:access-analyzer:${Region}:${Account}:analyzer/${AnalyzerName}`	aws:ResourceTag/${TagKey}
ArchiveRule	`arn:${Partition}:access-analyzer:${Region}:${Account}:analyzer/${AnalyzerName}/archive-rule/${RuleName}`	

Bedingungsschlüssel für AWS IAM Access Analyzer

AWS IAM Access Analyzer definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung.	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf den Tag-Schlüssel-Wert-Paaren, die an die Ressource angefügt wurden.	Zeichenfolge
aws:TagKeys	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Zustandsschlüssel für AWS IAM Identity Center (Nachfolger von AWS Single Sign-On)

AWS IAM Identity Center (Nachfolger von AWS Single Sign-On) (Service-Präfix: `sso`) bietet die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS IAM Identity Center definierte Aktionen (Nachfolger von AWS Single Sign-On)

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateDirectory	Erteilung der Berechtigung zur Verbindung eines Verzeichnisses, das von AWS IAM Identity Center verwendet werden soll	Schreiben			ds:AuthorizeApplication
AssociateProfile	Gewährt die Berechtigung zum Erstellen einer Verknüpfung zwischen einem Verzeichnisbenutzer oder einer Gruppe und einem Profil	Schreiben			
AttachCustomerManagedPolicyReferenceToPermissionSet	Erteilung der Berechtigung, einen Verweis auf eine vom Kunden verwaltete Richtlinie an einen Berechtigungssatz anzuhängen	Berechtigungsverwaltung	Instance* PermissionSet*		
AttachManagedPolicyToPermissionSet	Gewährt die Berechtigung zum Anhängen einer von AWS verwalteten Richtlinie an einen Berechtigungssatz	Berechtigungsverwaltung	Instance* PermissionSet*		
CreateAccountAssignment	Gewährt die Berechtigung, einem AWS-Konto mit einem bestimmten Berechtigungssatz	Schreiben	Account* Instance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	den Zugriff auf einen Prinzipal zuzuweisen		PermissionSet*		
CreateApplication	Gewährt die Berechtigung zum Erstellen einer Anwendung	Schreiben	ApplicationProvider*		
			Instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateApplicationAssignment	Gewährt die Berechtigung zum Erstellen einer Anwendungszuweisung	Schreiben	Application*		
				sso:ApplicationAccount	
CreateApplicationInstance	Erteilung der Berechtigung zum Hinzufügen einer Anwendungs-Instance zum AWS IAM Identity Center	Schreiben			
CreateApplicationInstanceCertificate	Gewährt die Berechtigung zum Hinzufügen eines neuen Zertifikats für eine Anwendungsinstance	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateInstance	Gewährt die Berechtigung zum Erstellen einer Identity Center-Instance	Schreiben	Instance*		iam:CreateServiceLinkedRole organizations:DescribeOrganization
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateInstanceAccessControlAttributeConfiguration	Gewährt die Berechtigung, die Instance für ABAC zu aktivieren und die Attribute anzugeben	Schreiben	Instance*		iam:AttachRolePolicy iam:CreateRole iam:DeleteRole iam:DeleteRolePolicy iam:DetachRolePolicy iam:GetRole iam:ListAttachedRolePolicies iam:ListRolePolicies iam:PutRolePolicy

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					iam:UpdateAssumeRolePolicy
CreateManagedApplicationInstance	Erteilung der Berechtigung zum Hinzufügen einer verwalteten Anwendungs-Instance zum AWS IAM Identity Center	Schreiben			
CreatePermissionSet	Gewährt die Berechtigung zum Erstellen eines Berechtigungssatzes	Write	Instance*		
			PermissionSet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfile	Gewährt die Berechtigung zum Erstellen eines Profils für eine Anwendungsinstance	Write			
CreateTrust	Gewährt die Berechtigung zum Erstellen einer Verbundvertrauensstellung in einem Zielkonto	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTrustedTokenIssuer	Gewährt die Berechtigung zum Erstellen eines vertrauenswürdigen Token-Ausstellers für eine Instance	Schreiben	Instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccountAssignment	Gewährt die Berechtigung, den Zugriff eines Prinzipals mit einem bestimmten Berechtigungssatz von einem AWS-Konto zu löschen	Schreiben	Account*		
			Instance*		
			PermissionSet*		
DeleteApplication	Gewährt die Berechtigung zum Löschen einer Anwendung	Schreiben	Application*		
				sso:ApplicationAccount	
DeleteApplicationAccessScope	Gewährt die Berechtigung zum Löschen des Zugriffsbereichs für eine Anwendung	Schreiben	Application*		
				sso:ApplicationAccount	
DeleteApplicationAssignment	Gewährt die Berechtigung zum Löschen einer Anwendungszuweisung	Schreiben	Application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				sso:ApplicationAccount	
DeleteApplicationAuthenticationMethod	Gewährt die Berechtigung zum Löschen einer Authentifizierungsmethode für eine Anwendung	Schreiben	Application*		
				sso:ApplicationAccount	
DeleteApplicationGrant	Gewährt die Berechtigung zum Löschen einer Erteilung aus einer Anwendung	Schreiben	Application*		
				sso:ApplicationAccount	
DeleteApplicationInstance	Gewährt die Berechtigung zum Löschen der Anwendungsinstance	Write			
DeleteApplicationInstanceCertificate	Inaktives oder abgelaufenes Zertifikat aus der App-Instance löschen	Schreiben			
DeleteInlinePolicyFromPermissionSet	Gewährt die Berechtigung zum Löschen der Inline-Richtlinie aus einem angegebenen Berechtigungssatz	Schreiben	Instance*		
			PermissionSet*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteInstance	Gewährt die Berechtigung zum Löschen einer Identity Center-Instance	Schreiben	Instance*		
DeleteInstanceAccessControlAttributeConfiguration	Gewährt die Berechtigung, ABAC zu deaktivieren und die Attributliste für die Instance zu entfernen	Write	Instance*		
DeleteManagedApplicationInstance	Gewährt die Berechtigung zum Löschen der verwalteten Anwendungsinstance	Write			
DeletePermissionSet	Gewährt die Berechtigung zum Löschen eines Berechtigungssatzes	Schreiben	Instance* PermissionSet*		
DeletePermissionsBoundaryFromPermissionSet	Erteilung der Berechtigung zum Entfernen von Berechtigungsgrenzen aus einer Berechtigungsgruppe	Berechtigungsverwaltung	Instance* PermissionSet*		
DeletePermissionsPolicy	Gewährt die Berechtigung zum Löschen der mit einem Berechtigungssatz verknüpften Berechtigungsrichtlinie	Berechtigungsverwaltung			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteProfile	Gewährt die Berechtigung zum Löschen des Profils für eine Anwendungsinstance	Schreiben			
DeleteTrustedTokenIssuer	Gewährt die Berechtigung zum Löschen eines vertrauenswürdigen Token-Ausstellers für eine Instance	Schreiben	TrustedTokenIssuer*		
DescribeAccountAssignmentCreationStatus	Gewährt die Berechtigung, den Status der Anforderung zur Zuordnungserstellung zu beschreiben	Lesen	Instance*		
DescribeAccountAssignmentDeletionStatus	Gewährt die Berechtigung, den Status einer Anforderung zur Zuordnungslöschung zu beschreiben	Lesen	Instance*		
DescribeApplication	Gewährt die Berechtigung zum Erhalten von Informationen zu einer Anwendung	Lesen	Application*		
				sso:ApplicationAccount	
DescribeApplicationAssignment	Gewährt die Berechtigung zum Abrufen einer Anwendungszuweisung	Lesen	Application*		
				sso:ApplicationAccount	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeApplicationProvider	Gewährt die Berechtigung zum Beschreiben einer Anwendungsanbieters	Lesen	ApplicationProvider*		
DescribeDirectories	Gewährt die Berechtigung zum Erhalten von Informationen über die Verzeichnisse für dieses Konto	Lesen			
DescribeInstance	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Identity Center-Instance	Lesen	Instance*		
DescribeInstanceAccessControlAttributeConfiguration	Gewährt die Berechtigung, die Liste der Attribute abzurufen, die von der Instance für ABAC verwendet werden	Read	Instance*		
DescribePermissionSet	Gewährt die Berechtigung zur Beschreibung eines Berechtigungssatzes	Lesen	Instance* PermissionSet*		
DescribePermissionSetProvisioningStatus	Gewährt die Berechtigung zum Beschreiben des Status für die angegebene Bereitstellungsanforderung für Berechtigungssätze	Lesen	Instance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribePermissionsPolicies	Gewährt die Berechtigung zum Abrufen aller mit einem Berechtigungssatz verknüpften Berechtigungsrichtlinien	Lesen			
DescribeRegisteredRegions	Erteilung der Berechtigung, die Regionen zu erhalten, in denen Ihr Unternehmen AWS IAM Identity Center aktiviert hat	Lesen			
DescribeTrustedTokenIssuer	Gewährt die Berechtigung zum Beschreiben eines vertrauenswürdigen Token-Ausstellers für eine Instance	Lesen	TrustedTokenIssuer*		
DescribeTrusts	Gewährt die Berechtigung zum Erhalten von Informationen über die Vertrauensstellungen für dieses Konto	Lesen			
DetachCustomerManagedPolicyReferenceFromPermissionSet	Erteilung der Berechtigung zum Trennen eines Verweises auf eine vom Kunden verwaltete Richtlinie von einem Berechtigungssatz	Berechtigungsverwaltung	Instance* PermissionSet*		
DetachManagedPolicyFromPermissionSet	Gewährt die Berechtigung, die verwaltete AWS-Richtlinie vom angegebenen Berechtigungssatz zu trennen	Berechtigungsverwaltung	Instance* PermissionSet*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateDirectory	Erteilung der Berechtigung zum Trennen eines Verzeichnisses, das von AWS IAM Identity Center verwendet werden soll	Schreiben			ds:UnauthorizeApplication
DisassociateProfile	Gewährt die Berechtigung, einen Verzeichnisbenutzer oder eine Gruppe von einem Profil zu trennen	Schreiben			
GetApplicationAccessScope	Gewährt die Berechtigung zum Erhalten eines Zugriffsbereichs für eine Anwendung	Lesen	Application*		
				sso:ApplicationAccount	
GetApplicationAssignmentConfiguration	Gewährt die Berechtigung Zuweisungskonfigurationen für eine Anwendung zu lesen	Lesen	Application*		
				sso:ApplicationAccount	
GetApplicationAuthenticationMethod	Gewährt die Berechtigung zum Erhalten einer Authentifizierungsmethode für eine Anwendung	Lesen	Application*		
				sso:ApplicationAccount	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetApplicationGrant	Gewährt die Berechtigung, Einzelheiten zu einem Zuschuss abzurufen, der zu einer Anwendung gehört	Lesen	Application*		
				sso:ApplicationAccount	
GetApplicationInstance	Gewährt die Berechtigung zum Abrufen von Details für eine Anwendungsinstance	Read			
GetApplicationTemplate	Gewährt die Berechtigung zum Abrufen von Details zur Anwendungsvorlage	Lesen			
GetInlinePolicyForPermissionSet	Gewährt die Berechtigung zum Abrufen der Inline-Richtlinie, die dem Berechtigungssatz zugewiesen ist	Lesen	Instance*		
			PermissionSet*		
GetManagedApplicationInstance	Gewährt die Berechtigung zum Abrufen von Details für eine Anwendungsinstance	Read			
GetMfaDeviceManagementForDirectory	Gewährt die Berechtigung zum Abrufen von Einstellungen für die Verwaltung von Mfa Device Management für das Verzeichnis	Read			
GetPermissionSet	Gewährt die Berechtigung zum Abrufen von Details eines Berechtigungssatzes	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetPermissionsBoundaryForPermissionSet	Erteilung der Berechtigung zum Abrufen der Berechtigungsgrenze für eine Berechtigungsgruppe	Lesen	Instance*		
			PermissionSet*		
GetPermissionsPolicy	Gewährt die Berechtigung zum Abrufen aller mit einem Berechtigungssatz verknüpften Berechtigungsrichtlinien	Read			sso:DescribePermissionsPolicies
GetProfile	Gewährt die Berechtigung zum Abrufen eines Profils für eine Anwendungsinstance	Lesen			
GetSSOStatus	Ermöglicht die Überprüfung, ob das AWS IAM Identity Center aktiviert ist	Lesen			
GetSharedSsoConfiguration	Gewährt die Berechtigung zum Abrufen der gemeinsam genutzten Konfiguration für die aktuelle SSO-Instance	Read			
GetSsoConfiguration	Gewährt die Berechtigung zum Abrufen der Konfiguration für die aktuelle SSO-Instance	Read			
GetTrust	Gewährt die Berechtigung, die Verbundvertrauensstellung in ein Zielkonto abzurufen	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ImportApplicationInstanceServiceProviderMetadata	Gewährt die Berechtigung, die Anwendungsinstance durch Hochladen einer vom Serviceanbieter bereitgestellten Anwendungs-SAML-Metadatendatei zu aktualisieren	Schreiben			
ListAccountAssignmentCreationStatus	Gewährt die Berechtigung, den Status der AWS-Konto-Anforderungen zur Zuordnungserstellung für eine bestimmte SSO-Instance aufzulisten	Auflisten	Instance*		
ListAccountAssignmentDeletionStatus	Gewährt die Berechtigung, den Status der AWS-Konto-Anforderungen zur Zuordnungslöschung für eine bestimmte SSO-Instance aufzulisten	Auflisten	Instance*		
ListAccountAssignments	Gewährt die Berechtigung, den Beauftragten des angegebenen AWS-Konto mit dem angegebenen Berechtigungssatz aufzulisten	Auflisten	Account*		
			Instance*		
			PermissionSet*		
ListAccountAssignmentsForPrincipal	Gewährt die Berechtigung, Konten aufzulisten, die einem Benutzer oder einer Gruppe zugewiesen sind	Auflisten	Instance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAccountsForProvisionedPermissionSet	Gewährt die Berechtigung, alle AWS-Konten aufzulisten, in denen der angegebene Berechtigungssatz bereitgestellt wird	Auflisten	Instance*		
			PermissionSet*		
ListApplicationAccessScopes	Gewährt die Berechtigung zum Auflisten von Zugriffsbereichen für eine Anwendung	Auflisten	Application*		
				sso:ApplicationAccount	
ListApplicationAssignments	Gewährt die Berechtigung zum Auflisten von Anwendungszuordnungen	Auflisten	Application*		
				sso:ApplicationAccount	
ListApplicationAssignmentsForPrincipal	Gewährt die Berechtigung zum Auflisten von Anwendungen, die einem Benutzer oder einer Gruppe zugewiesen sind	Auflisten	Instance*		
				sso:ApplicationAccount	
ListApplicationAuthenticationMethods	Gewährt die Berechtigung zum Auflisten von Authentifizierungsmethoden für eine Anwendung	Auflisten	Application*		
				sso:ApplicationAccount	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListApplicationGrants	Gewährt die Berechtigung zum Auflisten von Berechtigungserteilungen einer Anwendung	Auflisten	Application*		
				sso:ApplicationAccount	
ListApplicationInstanceCertificates	Gewährt die Erlaubnis, alle Zertifikate für eine bestimmte Anwendungsinstance abzurufen	Read			
ListApplicationInstances	Gewährt die Berechtigung zum Abrufen aller Anwendungsinstanceen	Auflisten			sso:GetApplicationInstance
ListApplicationProviders	Gewährt die Berechtigung zum Auflisten von Anwendungsanbietern	Auflisten	ApplicationProvider*		
ListApplicationTemplates	Gewährt die Berechtigung zum Abrufen aller unterstützten Anwendungsvorlagen	Auflisten			sso:GetApplicationTemplate
ListApplications	Gewährt die Berechtigung zum Abrufen aller Anwendungen, die der Instance von IAM Identity Center zugeordnet sind	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListCustomerManagedPolicyReferencesInPermissionSet	Ermöglicht die Auflistung der vom Kunden verwalteten Richtlinien, die mit einem Berechtigungssatz verbunden sind	Auflisten	Instance* PermissionSet*		
ListDirectoryAssociations	Erteilung der Berechtigung zum Abrufen von Details über das mit dem AWS IAM Identity Center verbundene Verzeichnis	Lesen			
ListInstances	Gewährt die Berechtigung, die SSO-Instances aufzulisten, auf die der Anrufer Zugriff hat	Auflisten			
ListManagedPoliciesInPermissionSet	Gewährt die Berechtigung zum Auflisten der von AWS verwalteten Richtlinien, die einem bestimmten Berechtigungssatz angefügt sind	Auflisten	Instance* PermissionSet*		
ListPermissionSetProvisioningStatus	Gewährt die Berechtigung, den Status der Bereitstellungsanforderungen für Berechtigungssätze für eine bestimmte SSO-Instance aufzulisten	Auflisten	Instance*		
ListPermissionSets	Gewährt die Berechtigung zum Abrufen aller Berechtigungssätze	Auflisten	Instance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListPermissionSetsProvisionedToAccount	Gewährt die Berechtigung, alle Berechtigungssätze aufzulisten, die für ein bestimmtes AWS-Konto bereitgestellt sind	Auflisten	Account*		
			Instance*		
ListProfileAssociations	Gewährt die Berechtigung zum Abrufen des Verzeichnisbenutzers oder der Verzeichnisgruppe, die mit dem Profil verknüpft ist	Read			
ListProfiles	Gewährt die Berechtigung zum Abrufen aller Profile für eine Anwendungsinstance	Auflisten			sso:GetProfile
ListTagsForResource	Gewährt die Berechtigung, die Tags aufzulisten, die einer bestimmten Ressource angefügt sind	Lesen	Application		
			Instance		
			PermissionSet		
			TrustedTokenIssuer		
ListTrustedTokenIssuers	Gewährt die Berechtigung, vertrauenswürdige Token-Emittenten für eine Instance aufzulisten	Auflisten	Instance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ProvisionPermissionSet	Gewährt die Berechtigung zum Bereitstellen eines angegebenen Berechtigungssatzes für das angegebene Ziel	Schreiben	Account*		
			Instance*		
			PermissionSet*		
PutApplicationAccessScope	Gewährt die Berechtigung, einen Zugriffsbereich für eine Anwendung zu erstellen/zu aktualisieren	Schreiben	Application*		
				sso:ApplicationAccount	
PutApplicationAssignmentConfiguration	Gewährt die Berechtigung, einer Anwendung Zuweisungskonfigurationen hinzuzufügen	Schreiben	Application*		
				sso:ApplicationAccount	
PutApplicationAuthenticationMethod	Gewährt die Berechtigung zum Erstellen/Aktualisieren einer Authentifizierungsmethode für eine Anwendung	Schreiben	Application*		
				sso:ApplicationAccount	
PutApplicationGrant	Gewährt die Berechtigung zum Erstellen/Aktualisieren einer Zuwendung für eine Anwendung	Schreiben	Application*		
				sso:ApplicationAccount	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutInlinePolicyToPermissionSet	Gewährt die Berechtigung zum Anfügen einer IAM-Inline-Richtlinie an einen Berechtigungssatz	Schreiben	Instance*		
			PermissionSet*		
PutMfaDeviceManagementForDirectory	Gewährt die Berechtigung, Mfa Device Management-Einstellungen für das Verzeichnis zu erstellen	Schreiben			
PutPermissionsBoundaryToPermissionSet	Erteilung der Berechtigung zum Hinzufügen von Berechtigungsgrenzen zu einer Berechtigungsgruppe	Berechtigungsverwaltung	Instance*		
			PermissionSet*		
PutPermissionsPolicy	Gewährt die Berechtigung zum Hinzufügen einer Richtlinie zu einem Berechtigungssatz	Berechtigungsverwaltung			
SearchGroups	Gewährt die Berechtigung zur Suche nach Gruppen innerhalb des zugeordneten Verzeichnisses	Read			ds:DescribeDirectories
SearchUsers	Gewährt die Berechtigung zur Suche nach Benutzern innerhalb des zugeordneten Verzeichnisses	Lesen			ds:DescribeDirectories

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartSSO	Erteilung der Erlaubnis zur Initialisierung des AWS IAM Identity Center	Schreiben			organizations:DescribeOrganization organizations:EnableAWSServiceAccess
TagResource	Gewährt die Berechtigung, eine Gruppe von Tags mit einer bestimmten Ressource zu verknüpfen	Tagging	Application		
			Instance		
			PermissionSet		
			TrustedTokenIssuer		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung, die Verknüpfung einer Gruppe von Tags mit einer bestimmten Ressource aufzuheben	Tagging	Application		
			Instance		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			PermissionSet		
			TrustedTokenIssuer		
				aws:TagKeys	
UpdateApplication	Gewährt die Berechtigung zum Aktualisieren einer Anwendung	Schreiben	Application*		
				sso:ApplicationAccount	
UpdateApplicationInstanceActiveCertificate	Gewährt die Berechtigung zum Festlegen eines Zertifikats als aktives für diese Anwendungsinstance	Write			
UpdateApplicationInstanceDisplayData	Gewährt die Berechtigung zum Aktualisieren von Anzeigedaten einer Anwendungsinstance	Write			
UpdateApplicationInstanceResponseConfiguration	Gewährt die Berechtigung zum Aktualisieren der Verbundantwortkonfiguration für die Anwendungsinstance	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateApplicationInstanceResponseSchemaConfiguration	Gewährt die Berechtigung zum Aktualisieren der Verbundantwortschemakonfiguration für die Anwendungsinstance	Write			
UpdateApplicationInstanceSecurityConfiguration	Gewährt die Berechtigung zum Aktualisieren von Sicherheitsdetails für die Anwendungsinstance	Write			
UpdateApplicationInstanceServiceProviderConfiguration	Gewährt die Berechtigung zum Aktualisieren der Serviceanbieterbezogene Konfiguration für die Anwendungsinstance	Write			
UpdateApplicationInstanceStatus	Gewährt die Berechtigung, den Status einer Anwendungsinstance zu aktualisieren	Write			
UpdateDirectoryAssociation	Gewährt die Berechtigung zum Aktualisieren der Benutzerattributzuweisungen für Ihr verbundenes Verzeichnis	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateInstance	Gewährt die Berechtigung zum Aktualisieren einer Identity Center-Instance	Schreiben	Instance*		
UpdateInstanceAccessControlAttributeConfiguration	Gewährt die Berechtigung zum Aktualisieren der Attribute, die mit der Instance für ABAC verwendet werden sollen	Write	Instance*		
UpdateManagedApplicationInstanceStatus	Gewährt die Berechtigung zum Aktualisieren des Status einer verwalteten Anwendungsinstance	Schreiben			
UpdatePermissionSet	Gewährt die Berechtigung zum Aktualisieren des Berechtigungssatzes	Berechtigungsverwaltung	Instance* PermissionSet*		
UpdateProfile	Gewährt die Berechtigung zum Aktualisieren des Profils für eine Anwendungsinstance	Write			
UpdateSSOConfiguration	Gewährt die Berechtigung zum Aktualisieren der Konfiguration für die aktuelle SSO-Instance	Write			
UpdateTrust	Gewährt die Berechtigung, die Verbundvertrauensstellung in einem Zielkonto zu aktualisieren	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateTrustedTokenIssuer	Gewährt die Berechtigung zum Aktualisieren eines vertrauenswürdigen Token-Ausstellers für eine Instance	Schreiben	TrustedTokenIssuer *		

Von AWS IAM Identity Center (Nachfolger von AWS Single Sign-On) definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
PermissionSet	`arn:${Partition}:sso:::permissionSet/${InstanceId}/${PermissionSetId}`	aws:ResourceTag/${TagKey}
Account	`arn:${Partition}:sso:::account/${AccountId}`	
Instance	`arn:${Partition}:sso:::instance/${InstanceId}`	aws:ResourceTag/${TagKey}
Application	`arn:${Partition}:sso::${AccountId}:application/${InstanceId}/${ApplicationId}`	aws:ResourceTag/${TagKey} sso:ApplicationAccount

Ressourcentypen	ARN	Bedingungsschlüssel
TrustedTokenIssuer	`arn:${Partition}:sso::${AccountId}:trustedTokenIssuer/${InstanceId}/${TrustedTokenIssuerId}`	aws:ResourceTag/${TagKey}
ApplicationProvider	`arn:${Partition}:sso::aws:applicationProvider/${ApplicationProviderId}`	

Bedingungsschlüssel für AWS IAM Identity Center (Nachfolger von AWS Single Sign-On)

AWS IAM Identity Center (Nachfolger von AWS Single Sign-On) definiert die folgenden Bedingungsschlüssel, die in einem `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString
sso:ApplicationAccount	Filtert den Zugriff nach dem Konto, das die Anwendung erstellt	String

Aktionen, Ressourcen und Bedingungsschlüssel für AWS IAM Identity Center (Nachfolger von AWS Single Sign-On)-Directory

AWS IAM Identity Center (Nachfolger von AWS Single Sign-On)-Directory (Service-Präfix: `sso-directory`) bietet die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS IAM Identity Center (Nachfolger von AWS Single Sign-On)-Directory definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden.

Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddMemberToGroup	Gewährt die Berechtigung zum Hinzufügen eines Mitglieds zu einer Gruppe in dem standardmäßig von AWS IAM Identity Center bereitgestellten Verzeichnis	Schreiben			
CompleteVirtualMfaDeviceRegistration	Gewährt die Berechtigung zum Abschließen des Erstellungsprozesses eines virtuellen MFA-Geräts	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CompleteWebAuthnDeviceRegistration	Gewährt die Berechtigung, den Registrierungsprozess eines WebAuthn-Geräts abzuschließen	Schreiben			
CreateAlias	Gewährt die Berechtigung zum Erstellen eines Alias für das standardmäßig von AWS IAM Identity Center bereitgestellte Verzeichnis	Schreiben			
CreateBearerToken	Gewährt die Berechtigung zum Erstellen eines Bearer-Tokens für einen bestimmten Bereitstellungsmandanten	Write			
CreateExternalIdPConfigurationForDirectory	Gewährt die Berechtigung zum Erstellen einer Konfiguration für einen externen Identitätsanbieter für das Verzeichnis	Schreiben			
CreateGroup	Gewährt die Berechtigung zum Erstellen einer Gruppe in dem standardmäßig von AWS IAM Identity Center bereitgestellten Verzeichnis	Schreiben			
CreateProvisioningTenant	Gewährt die Berechtigung zum Erstellen eines Bereitstellungsmandanten für ein bestimmtes Verzeichnis	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateUser	Gewährt die Berechtigung zum Erstellen eines Benutzers in dem standardmäßig von AWS IAM Identity Center bereitgestellten Verzeichnis	Schreiben			
DeleteBearerToken	Gewährt die Berechtigung zum Löschen eines Inhaber-Tokens	Write			
DeleteExternalIdPCertificate	Gewährt die Berechtigung zum Löschen des angegebenen externen IdP-Zertifikats	Write			
DeleteExternalIdPConfigurationForDirectory	Gewährt die Berechtigung zum Löschen einer Konfiguration für einen externen Identitätsanbieter, die dem Verzeichnis zugeordnet ist	Schreiben			
DeleteGroup	Gewährt die Berechtigung zum Löschen einer Gruppe aus dem standardmäßig von AWS IAM Identity Center bereitgestellten Verzeichnis	Schreiben			
DeleteMfaDeviceForUser	Gewährt die Berechtigung zum Löschen eines MFA-Geräts nach Gerätenamen für einen bestimmten Benutzer	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteProvisioningTenant	Gewährt die Berechtigung zum Löschen des Bereitstellungsmandanten	Schreiben			
DeleteUser	Gewährt die Berechtigung zum Löschen eines Benutzers aus dem standardmäßig von AWS IAM Identity Center bereitgestellten Verzeichnis	Schreiben			
DescribeDirectory	Gewährt die Berechtigung zum Abrufen von Informationen über das standardmäßig von AWS IAM Identity Center bereitgestellte Verzeichnis	Lesen			
DescribeGroup	Gewährt die Berechtigung zum Abfragen der Gruppendaten, einschließlich Benutzer- und Gruppenmitgliedern	Lesen			
DescribeGroups	Gewährt die Berechtigung zum Abrufen von Informationen über Gruppen aus dem von AWS IAM Identity Center standardmäßig bereitgestellten Verzeichnis	Lesen			
DescribeProvisioningTenant	Gewährt die Erlaubnis zur Beschreibung des bereitstellenden Mieters	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeUser	Gewährt die Berechtigung zum Abrufen von Informationen über einen Benutzer aus dem von AWS IAM Identity Center standardmäßig bereitgestellten Verzeichnis	Lesen			
DescribeUserByUniqueAttribute	Gewährt die Berechtigung, Benutzer mit einem gültigen eindeutigen Attribut zu beschreiben, das für den Benutzer dargestellt wird	Lesen			
DescribeUsers	Gewährt die Berechtigung zum Abrufen von Informationen über Benutzer aus dem von AWS IAM Identity Center standardmäßig bereitgestellten Verzeichnis	Lesen			
DisableExternalIdPConfigurationForDirectory	Gewährt die Berechtigung zum Deaktivieren der Authentifizierung von Endbenutzern mit einem externen Identitätsanbieter.	Schreiben			
DisableUser	Gewährt die Berechtigung zum Deaktivieren eines Benutzers in dem standardmäßig von AWS IAM Identity Center bereitgestellten Verzeichnis	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
EnableExternalIdPConfigurationForDirectory	Gewährt die Berechtigung zur Authentifizierung von Endbenutzern mit einem externen Identitätsanbieter	Schreiben			
EnableUser	Gewährt die Berechtigung zum Aktivieren eines Benutzers in dem standardmäßig von AWS IAM Identity Center bereitgestellten Verzeichnis	Schreiben			
GetAWSSPConfigurationForDirectory	Gewährt die Berechtigung zum Abrufen der AWS IAM Identity Center-Serviceanbieter-Konfigurationen für das Verzeichnis	Lesen			
GetUserPoolInfo	Gewährt die Berechtigung zum Abrufen von UserPool Inf	Lesen			
ImportExternalIdPCertificate	Gewährt die Berechtigung zum Importieren des IdP-Zertifikats, das zum Überprüfen externer IdP-Antworten verwendet wird	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
IsMemberInGroup	Gewährt die Berechtigung zu prüfen, ob ein Mitglied Teil der Gruppe in dem standardmäßig von AWS IAM Identity Center bereitgestellten Verzeichnisses ist	Lesen			
ListBearerTokens	Gewährt die Berechtigung zum Auflisten von Bearer-Token für einen bestimmten Bereitstellungsmandanten	Read			
ListExternalIdPCertificates	Gewährt die Berechtigung zum Auflisten der externen Identitätsanbieterzertifikate eines bestimmten Verzeichnisses und Identitätsanbieters	Read			
ListExternalIdPConfigurationsForDirectory	Gewährt die Berechtigung zum Auflisten aller für das Verzeichnis erstellten Konfigurationen für externe Identitätsanbieter	Read			
ListGroupsForMember	Gewährt die Berechtigung zum Auflisten von Gruppen des Zielmitglieds	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListGroupsForUser	Gewährt die Berechtigung zum Auflisten von Gruppen für einen Benutzer aus dem standardmäßig von AWS IAM Identity Center bereitgestellten Verzeichnis	Lesen			
ListMembersInGroup	Gewährt die Berechtigung zum Abrufen aller Mitglieder, die Teil einer Gruppe in dem standardmäßig von AWS IAM Identity Center bereitgestellten Verzeichnis	Lesen			
ListMfaDevicesForUser	Gewährt die Berechtigung zum Auflisten aller aktiven MFA-Geräte und ihrer MFA-Gerätemetadaten für einen Benutzer	Read			
ListProvisioningTenants	Gewährt die Berechtigung zum Auflisten von Bereitstellungsmandanten für ein bestimmtes Verzeichnis	Lesen			
RemoveMemberFromGroup	Gewährt die Berechtigung zum Entfernen eines Mitglieds, das Teil einer Gruppe in dem standardmäßig von AWS IAM Identity Center bereitgestellten Verzeichnis ist	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SearchGroups	Gewährt die Berechtigung zur Suche nach Gruppen innerhalb des zugeordneten Verzeichnisses	Read			
SearchUsers	Gewährt die Berechtigung zur Suche nach Benutzern innerhalb des zugeordneten Verzeichnisses	Read			
StartVirtualMfaDeviceRegistration	Gewährt die Berechtigung zum Starten des Erstellungsprozesses eines virtuellen MFA-Geräts	Write			
StartWebAuthnDeviceRegistration	Gewährt die Berechtigung, den Registrierungsprozess eines WebAuthn-Geräts zu starten	Write			
UpdateExternalIdPConfigurationForDirectory	Gewährt die Berechtigung zum Aktualisieren einer mit dem Verzeichnis verknüpften Konfiguration für externe Identitätsanbieter	Schreiben			
UpdateGroup	Gewährt die Berechtigung zum Aktualisieren von Informationen zu einer Gruppe in dem standardmäßig von AWS IAM Identity Center bereitgestellten Verzeichnis	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateGroupDisplayName	Gewährt die Berechtigung zum Aktualisieren der Antwort auf Anzeigenamen für Gruppennamen	Write			
UpdateMfaDeviceForUser	Gewährt die Berechtigung, MFA-Geräteinformationen zu aktualisieren	Schreiben			
UpdatePassword	Gewährt die Berechtigung zum Aktualisieren des Passworts, indem der Link zum Zurücksetzen des Passworts per E-Mail gesendet oder ein einmaliges Passwort für einen Benutzer in dem standardmäßig von AWS IAM Identity Center bereitgestellten Verzeichnis generiert wird	Schreiben			
UpdateUser	Gewährt die Berechtigung zum Aktualisieren von Benutzerinformationen in dem standardmäßig von AWS IAM Identity Center bereitgestellten Verzeichnis	Schreiben			
UpdateUserName	Gewährt die Berechtigung zum Aktualisieren der Antwort auf den Benutzernamen für den Benutzernamen	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
VerifyEmail	Gewährt die Berechtigung zum Verifizieren der E-Mail-Adresse eines Benutzers	Schreiben			

Von AWS IAM Identity Center (Nachfolger von AWS Single Sign-On)-Directory definierte Ressourcentypen

AWS IAM Identity Center (Nachfolger von AWS Single Sign-On)-Directory unterstützt das Angeben eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um Zugriff auf das AWS IAM Identity Center (Nachfolger von AWS Single Sign-On)-Directory zu erteilen, geben Sie `"Resource": "*"` in einer Richtlinie an.

Bedingungsschlüssel für AWS IAM Identity Center (Nachfolger von AWS Single Sign-On)-Directory

IAM Identity Center (Nachfolger von AWS SSO)-Directory umfasst keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS IAM Identity Center OIDC-Service

AWS IAM Identity Center OIDC-Service (Servicepräfix: `sso-oauth`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.

- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Aktionen, die durch den AWS IAM Identity Center OIDC-Service definiert sind

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTokenWithIAM	Gewährt die Berechtigung, OAuth/OIDC-Token für den Zugriff auf integrierte IAM Identity Center-Anwendungen zu erstellen	Schreiben	Application*		

Durch den IAM Identity Center OIDC-Service definierte Ressourcentypen AWS

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Application	`arn:${Partition}:sso::${AccountId}:application/${InstanceId}/${ApplicationId}`	

Bedingungsschlüssel für den AWS IAM Identity Center OIDC-Service

OIDC-Service besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Identity and Access Management (IAM)

AWS Identity And Access Management (IAM) (Service-Präfix: `iam`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Identity and Access Management (IAM) definierte Aktionen
- Von AWS Identity and Access Management (IAM) definierte Ressourcentypen
- Bedingungsschlüssel für AWS Identity and Access Management (IAM)

Von AWS Identity and Access Management (IAM) definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddClientIDToOpenIDConnectProvider	Gewährt die Berechtigung zum Hinzufügen einer neuen Client-ID (Zielgruppe) zur Liste der registrierten IDs für die angegebene IAM OpenID Connect (OIDC)-Anbieterressource.	Write	oidc-provider*		
AddRoleToInstanceProfile	Gewährt die Berechtigung zum Hinzufügen einer IAM-Rolle zum angegebenen Instance-Profil.	Write	instance-profile*		iam:PassRole
AddUserToGroup	Gewährt die Berechtigung zum Hinzufügen eines IAM-Benutzers zur angegebenen IAM-Gruppe.	Write	group*		
AttachGroupPolicy	Gewährt die Berechtigung zum Anfügen einer verwalteten Richtlinie an die angegebene IAM-Gruppe.	Berechtigungsverwaltung	group*		
				iam:PolicyARN	
AttachRolePolicy	Gewährt die Berechtigung zum Anfügen einer verwalteten Richtlinie zur angegebenen IAM-Rolle.	Berechtigungsverwaltung	role*		
				iam:PolicyARN iam:PermissionsBoundary	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AttachUserPolicy	Gewährt die Berechtigung zum Anfügen einer verwalteten Richtlinie an den angegebenen IAM-Benutzer.	Berechtigungsverwaltung	user*		
				iam:PolicyARN iam:PermissionsBoundary	
ChangePassword	Gewährt einem IAM-Benutzer die Berechtigung, sein eigenes Passwort zu ändern	Schreiben	user*		
CreateAccessKey	Gewährt die Berechtigung zum Erstellen eines Zugriffsschlüssels und eines geheimen Zugriffsschlüssels für den angegebenen IAM-Benutzer.	Write	user*		
CreateAccountAlias	Gewährt die Berechtigung zum Erstellen eines Alias für Ihr AWS-Konto	Write			
CreateGroup	Gewährt die Berechtigung zum Erstellen einer neuen Gruppe.	Write	group*		
CreateInstanceProfile	Gewährt die Berechtigung zum Erstellen eines neuen Instance-Profils.	Write	instance-profile*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateLoginProfile	Gewährt die Berechtigung zum Erstellen eines Passworts für den angegebenen IAM-Benutzer.	Write	user*		
CreateOpenIDConnectProvider	Gewährt die Berechtigung zum Erstellen einer IAM-Ressource, die einen Identitätsanbieter (IdP) beschreibt, der OpenID Connect (OIDC) unterstützt.	Write	oidc-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePolicy	Gewährt die Berechtigung zum Erstellen einer neuen verwalteten Richtlinie.	Berechtigungsverwaltung	policy*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreatePolicyVersion	Gewährt die Berechtigung zum Erstellen einer neuen Version der angegebenen verwalteten Richtlinie.	Berechtigungsverwaltung	policy*		
CreateRole	Gewährt die Berechtigung zum Erstellen einer neuen Rolle.	Write	role*		
				iam:PermissionsBoundary aws:TagKeys aws:RequestTag/${TagKey}	
CreateSAMLProvider	Gewährt die Berechtigung zum Erstellen einer IAM-Ressource, die einen Identitätsanbieter (IdP) beschreibt, der SAML 2.0 unterstützt.	Write	saml-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceLinkedRole	Gewährt die Berechtigung zum Erstellen einer IAM-Rolle, die einem AWS-Service erlaubt, in Ihrem Auftrag Aktionen auszuführen	Write	role*		
				iam:AWSServiceName	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateServiceSpecificCredential	Gewährt die Berechtigung zum Erstellen neuer servicespezifischer Anmeldedaten für einen IAM-Benutzer.	Write	user*		
CreateUser	Gewährt die Berechtigung zum Erstellen eines neuen IAM-Benutzers.	Write	user*		
				iam:PermissionsBoundary aws:TagKeys aws:RequestTag/${TagKey}	
CreateVirtualMFADevice	Gewährt die Berechtigung zum Erstellen eines neuen virtuellen MFA-Geräts.	Write	mfa*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeactivateMFADevice	Gewährt die Berechtigung zum Deaktivieren des angegebenen MFA-Geräts und zum Entfernen der Mapping zu dem IAM-Benutzer, für den sie ursprünglich aktiviert wurde.	Write	user*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteAccessKey	Gewährt die Berechtigung zum Löschen des Zugriffsschlüsselpaars, das dem angegebenen IAM-Benutzer zugeordnet ist.	Write	user*		
DeleteAccountAlias	Gewährt die Berechtigung zum Löschen des angegebenen AWS-Konto-Alias	Write			
DeleteAccountPasswordPolicy	Gewährt die Berechtigung zum Löschen der Passwortrichtlinie für das AWS-Konto	Berechtigungsverwaltung			
DeleteCloudFrontPublicKey	Gewährt die Berechtigung, einen vorhandenen öffentlichen CloudFront-Schlüssel zu löschen	Schreiben			
DeleteGroup	Gewährt die Berechtigung zum Löschen der angegebenen IAM-Gruppe.	Write	group*		
DeleteGroupPolicy	Gewährt die Berechtigung zum Löschen der angegebenen eingebundenen Richtlinie aus der Gruppe.	Berechtigungsverwaltung	group*		
DeleteInstanceProfile	Gewährt die Berechtigung zum Löschen des angegebenen Instance-Profils.	Write	instance-profile*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteLoginProfile	Gewährt die Berechtigung zum Löschen des Passworts für den angegebenen IAM-Benutzer.	Write	user*		
DeleteOpenIDConnectProvider	Gewährt die Berechtigung zum Löschen eines Ressourcenobjekts eines OpenID Connect-Identitätsanbieters (IdP) in IAM.	Write	oidc-provider*		
DeletePolicy	Gewährt die Berechtigung zum Löschen und Entfernen der angegebenen verwalteten Richtlinie aus allen IAM-Entitys (Benutzer, Gruppen oder Rollen), denen sie angefügt ist.	Berechtigungsverwaltung	policy*		
DeletePolicyVersion	Gewährt die Berechtigung zum Löschen einer Version der angegebenen verwalteten Richtlinie.	Berechtigungsverwaltung	policy*		
DeleteRole	Gewährt die Berechtigung zum Löschen der angegebenen Rolle.	Write	role*		
DeleteRolePermissionsBoundary	Gewährt die Berechtigung zum Entfernen der Berechtigungsgrenze aus einer Rolle.	Berechtigungsverwaltung	role*	iam:PermissionsBoundary	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteRolePolicy	Gewährt die Berechtigung zum Löschen der angegebenen eingebundenen Richtlinie aus der angegebenen Rolle.	Berechtigungsverwaltung	role*		
				iam:PermissionsBoundary	
DeleteSAMLProvider	Gewährt die Berechtigung zum Löschen einer SAML-Anbieterressource in IAM.	Write	saml-provider*		
DeleteSSHPublicKey	Gewährt die Berechtigung zum Löschen des angegebenen öffentlichen SSH-Schlüssels.	Write	user*		
DeleteServerCertificate	Gewährt die Berechtigung zum Löschen des angegebenen Serverzertifikats.	Write	server-certificate*		
DeleteServiceLinkedRole	Gewährt die Berechtigung zum Löschen einer IAM-Rolle, die mit einem bestimmten AWS-Service verknüpft ist, wenn der Service diese nicht mehr verwendet	Write	role*		
DeleteServiceSpecificCredential	Gewährt die Berechtigung zum Löschen der angegebenen servicespezifischen Anmeldedaten für einen IAM-Benutzer.	Write	user*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteSigningCertificate	Gewährt die Berechtigung zum Löschen eines Signaturzertifikats, das dem angegebenen IAM-Benutzer zugeordnet ist.	Write	user*		
DeleteUser	Gewährt die Berechtigung zum Löschen des angegebenen IAM-Benutzers.	Write	user*		
DeleteUserPermissionsBoundary	Gewährt die Berechtigung zum Entfernen der Berechtigungsgrenze des angegebenen IAM-Benutzers.	Berechtigungsverwaltung	user*		
				iam:PermissionsBoundary	
DeleteUserPolicy	Gewährt die Berechtigung zum Löschen der angegebenen eingebundenen Richtlinie eines IAM-Benutzers.	Berechtigungsverwaltung	user*		
				iam:PermissionsBoundary	
DeleteVirtualMFADevice	Gewährt die Berechtigung zum Löschen eines virtuellen MFA-Geräts.	Write	mfa		
			sms-mfa		
DetachGroupPolicy	Gewährt die Berechtigung zum Trennen einer verwalteten Richtlinie von der angegebenen IAM-Gruppe.	Berechtigungsverwaltung	group*		
				iam:PolicyARN	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DetachRolePolicy	Gewährt die Berechtigung zum Trennen einer verwalteten Richtlinie von der angegebenen Rolle.	Berechtigungsverwaltung	role*		
				iam:PolicyARN iam:PermissionsBoundary	
DetachUserPolicy	Gewährt die Berechtigung zum Trennen einer verwalteten Richtlinie vom angegebenen IAM-Benutzer.	Berechtigungsverwaltung	user*		
				iam:PolicyARN iam:PermissionsBoundary	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
EnableMFADevice	Gewährt die Berechtigung zum Aktivieren eines MFA-Geräts und zum Zuordnen des Geräts zum angegebenen IAM-Benutzer.	Write	user*		
				iam:RegisterSecurityKey iam:FIDO-FIPS-140-2-certification iam:FIDO-FIPS-140-3-certification iam:FIDO-certification	
GenerateCredentialReport	Gewährt die Berechtigung zum Generieren eines Berichts zu Anmeldeinformationen für das AWS-Konto	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GenerateOrganizationsAccessReport	Gewährt die Berechtigung zum Generieren eines Zugriffsberichts für eine AWS-Organizations-Entity	Read	access-report*		organizations:DescribePolicy organizations:ListChildren organizations:ListParents organizations:ListPoliciesForTarget organizations:ListRoots organizations:ListTargetsForPolicy
				iam:OrganizationsPolicyId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GenerateServiceLastAccessedDetails	Gewährt die Berechtigung zum Generieren eines Berichts zum letzten Service-Zugriffsdatums für eine IAM-Ressource.	Read	group*		
			policy*		
			role*		
			user*		
GetAccessKeyLastUsed	Gewährt die Berechtigung zum Abrufen von Informationen über den letzten Verwendungszeitpunkt des angegebenen Zugriffsschlüssels.	Read	user*		
GetAccountAuthorizationDetails	Gewährt die Berechtigung zum Abrufen von Informationen zu allen IAM-Benutzern, -Gruppen, -Rollen und -Richtlinien im AWS-Konto, einschließlich der Beziehungen untereinander	Lesen			
GetAccountEmailAddress	Gewährt die Berechtigung, die E-Mail-Adresse, die mit dem Konto verknüpft ist, abzurufen	Lesen			
GetAccountName	Gewährt die Berechtigung, den Kontonamen, der mit dem Konto verknüpft ist, abzurufen	Lesen			
GetAccountPasswordPolicy	Gewährt die Berechtigung zum Abrufen der Passwortrichtlinie für das AWS-Konto	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAccountSummary	Gewährt die Berechtigung zum Abrufen von Informationen zur IAM-Entity-Nutzung und zu IAM-Kontingenten im AWS-Konto	Auflisten			
GetCloudFrontPublicKey	Gewährt die Berechtigung, Informationen zum angegebenen öffentlichen CloudFront-Schlüssel abzurufen	Lesen			
GetContextKeysForCustomPolicy	Gewährt die Berechtigung zum Abrufen einer Liste aller Kontextschlüssel, auf die in der angegebenen Richtlinie Bezug genommen wird.	Read			
GetContextKeysForPrincipalPolicy	Gewährt die Berechtigung zum Abrufen einer Liste aller Kontextschlüssel, auf die in allen IAM-Richtlinien, die der angegebenen IAM-Identität (Benutzer, Gruppe oder Rolle) angefügt sind, Bezug genommen wird.	Read	group role user		
GetCredentialReport	Gewährt die Berechtigung zum Abrufen eines Berichts zu Anmeldeinformationen für das AWS-Konto	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetGroup	Gewährt die Berechtigung zum Abrufen einer Liste von IAM-Benutzern in der angegebenen IAM-Gruppe.	Read	group*		
GetGroupPolicy	Gewährt die Berechtigung zum Abrufen eines eingebundenen Richtliniendokuments, das in der angegebenen IAM-Gruppe eingebettet ist.	Read	group*		
GetInstanceProfile	Gewährt die Berechtigung zum Abrufen von Informationen zum angegebenen Instance-Profil, einschließlich Pfad, GUID, ARN und Rolle des Instance-Profils.	Read	instance-profile*		
GetLoginProfile	Gewährt die Berechtigung zum Abrufen des Erstellungsdatums des Benutzernamens und Passworts für den angegebenen IAM-Benutzer.	Auflisten	user*		
GetMFADevice	Gewährt dem angegebenen Benutzer die Berechtigung, Informationen zu einem MFA-Gerät abzurufen	Lesen	user*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetOpenIDConnectProvider	Gewährt die Berechtigung zum Abrufen von Informationen zur angegebenen OpenID Connect (OIDC)-Anbieterressource in IAM.	Read	oidc-provider*		
GetOrganizationsAccessReport	Gewährt die Berechtigung zum Abrufen eines AWS-Organizations-Zugriffsberichts	Read			
GetPolicy	Gewährt die Berechtigung zum Abrufen von Informationen zur angegebenen verwalteten Richtlinie, einschließlich Standardversion der Richtlinie und Gesamtzahl der Identitäten, denen die Richtlinie angefügt ist.	Read	policy*		
GetPolicyVersion	Gewährt die Berechtigung zum Abrufen von Informationen über eine Version der angegebenen verwalteten Richtlinie, einschließlich Richtliniendokument.	Read	policy*		
GetRole	Gewährt die Berechtigung zum Abrufen von Informationen zur angegebenen Rolle, einschließlich Pfad, GUID, ARN und Vertrauensrichtlinie der Rolle.	Read	role*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetRolePolicy	Gewährt die Berechtigung zum Abrufen eines eingebundenen Richtliniendokuments, das in der angegebenen IAM-Rolle eingebettet ist.	Read	role*		
GetSAMLProvider	Gewährt die Berechtigung zum Abrufen des SAML-Anbieter-Metadokuments, das beim Erstellen oder Aktualisieren der IAM-SAML-Anbieterressource hochgeladen wurde.	Read	saml-provider*		
GetSSHPublicKey	Gewährt die Berechtigung zum Abrufen des angegebenen öffentlichen SSH-Schlüssels, einschließlich Metadaten über den Schlüssel.	Read	user*		
GetServerCertificate	Gewährt die Berechtigung zum Abrufen von Informationen zum angegebenen Serverzertifikat, das in IAM gespeichert ist.	Read	server-certificate*		
GetServiceLastAccessedDetails	Gewährt die Berechtigung zum Abrufen von Informationen über den Bericht zum letzten Service-Zugriffsdatum.	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetServiceLastAccessedDetailsWithEntities	Gewährt die Berechtigung zum Abrufen von Informationen über die Entitys aus dem Bericht zum letzten Service-Zugriffsdatum.	Read			
GetServiceLinkedRoleDeletionStatus	Gewährt die Berechtigung zum Abrufen des Löschstatus einer mit dem IAM-Service verknüpften Rolle.	Read	role*		
GetUser	Gewährt die Berechtigung zum Abrufen von Informationen zum angegebenen IAM-Benutzer, einschließlich Erstellungsdatum, Pfad, eindeutiger ID und ARN des Benutzers.	Read	user*		
GetUserPolicy	Gewährt die Berechtigung zum Abrufen eines eingebundenen Richtliniendokuments, das für den angegebenen IAM-Benutzer eingebettet ist.	Read	user*		
ListAccessKeys	Gewährt die Berechtigung zum Auflisten der Informationen zu Zugriffsschlüssel-IDs, die dem angegebenen IAM-Benutzer zugeordnet sind.	List	user*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAccountAliases	Gewährt die Berechtigung zum Auflisten des Konto-Alias, das mit dem AWS-Konto verknüpft ist	List			
ListAttachedGroupPolicies	Gewährt die Berechtigung zum Auflisten aller verwalteten Richtlinien, die der angegebenen IAM-Gruppe zugeordnet sind.	List	group*		
ListAttachedRolePolicies	Gewährt die Berechtigung zum Auflisten aller verwalteten Richtlinien, die der angegebenen IAM-Rolle zugeordnet sind.	List	role*		
ListAttachedUserPolicies	Gewährt die Berechtigung zum Auflisten aller verwalteten Richtlinien, die dem angegebenen IAM-Benutzer zugeordnet sind.	Auflisten	user*		
ListCloudFrontPublicKeys	Gewährt die Berechtigung, alle aktuellen öffentlichen CloudFront-Schlüssel für das Konto aufzulisten	Auflisten			
ListEntitiesForPolicy	Gewährt die Berechtigung zum Auflisten aller IAM-Identitäten, denen die angegebene verwaltete Richtlinie angefügt ist.	List	policy*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListGroupPolicies	Gewährt die Berechtigung zum Auflisten der Namen der eingebundenen Richtlinien, die in der angegebenen IAM-Gruppe eingebettet sind.	List	group*		
ListGroups	Gewährt die Berechtigung zum Auflisten der IAM-Gruppen, die das angegebene Pfadpräfix enthalten.	List			
ListGroupsForUser	Gewährt die Berechtigung zum Auflisten der IAM-Gruppen, denen der angegebene IAM-Benutzer angehört.	List	user*		
ListInstanceProfileTags	Gewährt die Berechtigung zum Auflisten der Tags, die an das angegebene Instanceprofil angehängt sind	List	instance-profile*		
ListInstanceProfiles	Gewährt die Berechtigung zum Auflisten der Instance-Profile, die über das angegebene Pfadpräfix verfügen.	List			
ListInstanceProfilesForRole	Gewährt die Berechtigung zum Auflisten der Instance-Profile, denen die angegebene IAM-Rolle zugeordnet ist.	List	role*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListMFADeviceTags	Gewährt die Berechtigung zum Auflisten der Tags, die an das angegebene virtuelle mfa-Gerät angehängt sind	List	mfa*		
ListMFADevices	Gewährt die Berechtigung zum Auflisten der MFA-Geräte für einen IAM-Benutzer.	List	user		
ListOpenIDConnectProviderTags	Gewährt die Berechtigung zum Auflisten der Tags, die an den angegebenen OpenID Connect-Anbieter angehängt sind	List	oidc-provider*		
ListOpenIDConnectProviders	Gewährt die Berechtigung zum Auflisten von Informationen zu Ressourcenobjekten des IAM OpenID Connect (OIDC)-Anbieters, die im AWS-Konto definiert sind	List			
ListPolicies	Gewährt die Berechtigung zum Auflisten aller verwalteten Richtlinien.	List			
ListPoliciesGrantingServiceAccess	Gewährt die Berechtigung zum Aufführen von Informationen zu Richtlinien, die einer Entity Zugriff auf einen bestimmten Service gewähren.	List	group* role* user*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListPolicyTags	Gewährt die Berechtigung zum Auflisten der Tags, die an die angegebene verwaltete Richtlinie angehängt sind	List	policy*		
ListPolicyVersions	Gewährt die Berechtigung zum Auflisten von Informationen zu den Versionen der angegebenen verwalteten Richtlinie, einschließlich der Version, die derzeit die Standardversion der Richtlinie ist.	List	policy*		
ListRolePolicies	Gewährt die Berechtigung zum Auflisten der Namen der eingebundenen Richtlinien, die in die angegebene IAM-Rolle eingebettet sind.	List	role*		
ListRoleTags	Gewährt die Berechtigung zum Auflisten der Tags, die der angegebenen IAM-Rolle zugeordnet sind.	List	role*		
ListRoles	Gewährt die Berechtigung zum Auflisten der IAM-Rollen, die über das angegebene Pfadpräfix verfügen.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListSAMLProviderTags	Gewährt die Berechtigung zum Auflisten der Tags, die an den angegebenen SAML-Anbieter angehängt sind	List	saml-provider*		
ListSAMLProviders	Gewährt die Berechtigung zum Auflisten der SAML-Anbieterressourcen in IAM.	List			
ListSSHPublicKeys	Gewährt die Berechtigung zum Auflisten von Informationen zu den öffentlichen SSH-Schlüsseln, die dem angegebenen IAM-Benutzer zugeordnet sind.	Auflisten	user*		
ListSTSRegionalEndpointsStatus	Gewährt die Berechtigung zum Auflisten des Status aller aktiven regionalen STS-Endpunkte	Auflisten			
ListServerCertificateTags	Gewährt die Berechtigung zum Auflisten der Tags, die an das angegebene Serverzertifikat angehängt sind	List	server-certificate*		
ListServerCertificates	Gewährt die Berechtigung zum Auflisten der Server-Zertifikate, die über das angegebene Pfadpräfix verfügen.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListServiceSpecificCredentials	Gewährt die Berechtigung zum Auflisten der servicespezifischen Anmeldedaten, die dem angegebenen IAM-Benutzer zugeordnet sind.	List	user*		
ListSigningCertificates	Gewährt die Berechtigung zum Auflisten von Informationen zu den Signaturzertifikaten, die dem angegebenen IAM-Benutzer zugeordnet sind.	List	user*		
ListUserPolicies	Gewährt die Berechtigung zum Auflisten der Namen der eingebundenen Richtlinien, die für den angegebenen IAM-Benutzer eingebettet sind.	List	user*		
ListUserTags	Gewährt die Berechtigung zum Auflisten der Tags, die dem angegebenen IAM-Benutzer angefügt sind.	List	user*		
ListUsers	Gewährt die Berechtigung zum Auflisten der IAM-Benutzer, die über das angegebene Pfadpräfix verfügen.	List			
ListVirtualMFADevices	Gewährt die Berechtigung zum Auflisten von virtuellen MFA-Geräten nach Mappingsstatus.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PassRole [nur Berechtigung]	Gewährt die Berechtigung zum Übergeben einer Rolle an einen Service.	Write	role*		
				iam:AssociatedResourceArn iam:PassedToService	
PutGroupPolicy	Gewährt die Berechtigung zum Erstellen oder Aktualisieren eines eingebundenen Richtliniendokuments, das in die angegebene IAM-Gruppe eingebettet ist.	Berechtigungsverwaltung	group*		
PutRolePermissionsBoundary	Gewährt die Berechtigung zum Festlegen einer verwalteten Richtlinie als Berechtigungsgrenze für eine Rolle.	Berechtigungsverwaltung	role*		
				iam:PermissionsBoundary	
PutRolePolicy	Gewährt die Berechtigung zum Erstellen oder Aktualisieren eines eingebundenen Richtliniendokuments, das in der angegebenen IAM-Rolle eingebettet ist.	Berechtigungsverwaltung	role*		
				iam:PermissionsBoundary	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutUserPermissionsBoundary	Gewährt die Berechtigung zum Festlegen einer verwalteten Richtlinie als Berechtigungsgrenze für einen IAM-Benutzer.	Berechtigungsverwaltung	user*		
				iam:PermissionsBoundary	
PutUserPolicy	Gewährt die Berechtigung zum Erstellen oder Aktualisieren eines eingebundenen Richtliniendokuments, das für den angegebenen IAM-Benutzer eingebettet ist.	Berechtigungsverwaltung	user*		
				iam:PermissionsBoundary	
RemoveClientIDFromOpenIDConnectProvider	Gewährt die Berechtigung zum Entfernen der Client-ID (Zielgruppe) aus der Liste der Client-IDs in der angegebenen IAM OpenID Connect (OIDC)-Anbieterressource.	Write	oidc-provider*		
RemoveRoleFromInstanceProfile	Gewährt die Berechtigung zum Entfernen einer IAM-Rolle aus dem angegebenen EC2-Instance-Profil.	Write	instance-profile*		
RemoveUserFromGroup	Gewährt die Berechtigung zum Entfernen eines IAM-Benutzers aus der angegebenen Gruppe.	Write	group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ResetServiceSpecificCredential	Gewährt die Berechtigung zum Zurücksetzen des Passworts für vorhandene servicespezifische Anmeldedaten für einen IAM-Benutzer.	Write	user*		
ResyncMFADevice	Gewährt die Berechtigung zum Synchronisieren des angegebenen MFA-Geräts mit der IAM-Entity (Benutzer oder Rolle).	Write	user*		
SetDefaultPolicyVersion	Gewährt die Berechtigung zum Festlegen der Version der angegebenen Richtlinie als Standardversion der Richtlinie.	Berechtigungsverwaltung	policy*		
SetSTSRegionalEndpointStatus	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren eines regionalen STS-Endpunkts	Schreiben			
SetSecurityTokenServicePreferences	Gewährt die Berechtigung zum Festlegen der Tokenversion des globalen Endpunkts.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SimulateCustomPolicy	Gewährt die Berechtigung zum Simulieren, ob eine identitätsbasierte oder ressourcenbasierte Richtlinie Berechtigungen für bestimmte API-Produktionen und Ressourcen bereitstellt.	Read			
SimulatePrincipalPolicy	Gewährt die Berechtigung zum Simulieren, ob eine identitätsbasierte Richtlinie, die einer bestimmten IAM-Entity (Benutzer oder Rolle) Berechtigungen für bestimmte API-Produktionen und Ressourcen bereitstellt.	Read	group		
			role		
			user		
TagInstanceProfile	Gewährt die Berechtigung zum Hinzufügen von Tags zu einem Instanceprofil	Markieren	instance-profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagMFADevice	Gewährt die Berechtigung zum Hinzufügen von Tags zu einem virtuellen mfa-Gerät	Markieren	mfa*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
TagOpenIDConnectProvider	Gewährt die Berechtigung zum Hinzufügen von Tags zu einem OpenID Connect-Anbieter	Markieren	oidc-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagPolicy	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer verwalteten Richtlinie	Markieren	policy*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagRole	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer IAM-Rolle.	Markieren	role*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagSAMLProvider	Gewährt die Berechtigung zum Hinzufügen von Tags zu einem SAML-Anbieter	Markieren	saml-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagServerCertificate	Gewährt die Berechtigung zum Hinzufügen von Tags zu einem Serverzertifikat	Markieren	server-certificate*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagUser	Gewährt die Berechtigung zum Hinzufügen von Tags zu einem IAM-Benutzer.	Markieren	user*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagInstanceProfile	Gewährt die Berechtigung, die angegebenen Tags aus dem Instanceprofil zu entfernen	Markieren	instance-profile*		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UntagMFADevice	Gewährt die Berechtigung, die angegebenen Tags vom virtuellen mfa-Gerät zu entfernen	Markieren	mfa*		
				aws:TagKeys	
UntagOpenIDConnectProvider	Gewährt die Berechtigung, die angegebenen Tags vom OpenID Connect-Anbieter zu entfernen	Markieren	oidc-provider*		
				aws:TagKeys	
UntagPolicy	Gewährt die Berechtigung zum Entfernen der angegebenen Tags aus der verwalteten Richtlinie.	Markieren	policy*		
				aws:TagKeys	
UntagRole	Gewährt die Berechtigung zum Entfernen der angegebenen Tags aus der Rolle.	Markieren	role*		
				aws:TagKeys	
UntagSAMLProvider	Gewährt die Berechtigung, die angegebenen Tags vom SAML-Anbieter zu entfernen	Markieren	saml-provider*		
				aws:TagKeys	
UntagServerCertificate	Gewährt die Berechtigung, die angegebenen Tags aus dem Serverzertifikat zu entfernen	Markieren	server-certificate*		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UntagUser	Gewährt die Berechtigung zum Entfernen der angegebenen Tags aus dem Benutzerkonto.	Markieren	user*		
				aws:TagKeys	
UpdateAccessKey	Gewährt die Berechtigung zum Aktualisieren des Status des angegebenen Zugriffsschlüssels als „aktiv“ oder „inaktiv“.	Schreiben	user*		
UpdateAccountEmailAddress	Gewährt die Berechtigung, die E-Mail-Adresse, die mit dem Konto verknüpft ist, zu aktualisieren	Schreiben			
UpdateAccountName	Gewährt die Berechtigung, den Kontonamen, der mit dem Konto verknüpft ist, zu aktualisieren	Schreiben			
UpdateAccountPasswordPolicy	Gewährt die Berechtigung zum Aktualisieren der Passwortrichtlinien-Einstellungen für das AWS-Konto	Write			
UpdateAssumeRolePolicy	Gewährt die Berechtigung zum Aktualisieren der Richtlinie, die einer IAM-Entity die Berechtigung zum Annehmen einer Rolle gewährt.	Berechtigungsverwaltung	role*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateCloudFrontPublicKey	Gewährt die Berechtigung, einen vorhandenen öffentlichen CloudFront-Schlüssel zu aktualisieren	Schreiben			
UpdateGroup	Gewährt die Berechtigung zum Aktualisieren des Namens oder Pfads der angegebenen IAM-Gruppe.	Write	group*		
UpdateLoginProfile	Gewährt die Berechtigung zum Ändern des Passworts für den angegebenen IAM-Benutzer.	Write	user*		
UpdateOpenIDConnectProviderThumbprint	Gewährt die Berechtigung zum Aktualisieren der gesamten Liste der Serverzertifikat-Thumbprints, die einer OpenID Connect (OIDC)-Anbieterressource zugeordnet sind.	Write	oidc-provider*		
UpdateRole	Gewährt die Berechtigung zum Aktualisieren der Beschreibung oder der Einstellung für die maximale Sitzungsdauer einer Rolle.	Write	role*		
UpdateRoleDescription	Gewährt die Berechtigung zum Aktualisieren nur der Beschreibung einer Rolle.	Write	role*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateSAMLProvider	Gewährt die Berechtigung zum Aktualisieren des Metadatendokuments für eine vorhandene SAML-Anbieterressource.	Write	saml-provider*		
UpdateSSHPublicKey	Gewährt die Berechtigung zum Aktualisieren des Status eines öffentlichen SSH-Schlüssels eines IAM-Benutzers auf „Aktiv“ oder „Inaktiv“.	Write	user*		
UpdateServerCertificate	Gewährt die Berechtigung zum Aktualisieren des Namens oder Pfads des angegebenen Serverzertifikats, das in IAM gespeichert ist.	Write	server-certificate*		
UpdateServiceSpecificCredential	Gewährt die Berechtigung zum Aktualisieren von servicespezifischen Anmeldedaten für einen IAM-Benutzer auf „Aktiv“ oder „Inaktiv“.	Write	user*		
UpdateSigningCertificate	Gewährt die Berechtigung zum Aktualisieren des Status des Signaturzertifikats des angegebenen Benutzers auf „Aktiv“ oder „Inaktiv“.	Write	user*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateUser	Gewährt die Berechtigung zum Aktualisieren des Namens oder Pfads des angegebenen IAM-Benutzers.	Schreiben	user*		
UploadCloudFrontPublicKey	Gewährt die Berechtigung, einen vorhandenen öffentlichen CloudFront-Schlüssel hochzuladen	Schreiben			
UploadSSHPublicKey	Gewährt die Berechtigung zum Upload eines öffentlichen SSH-Schlüssels und zum Zuordnen des Schlüssels zum angegebenen IAM-Benutzer.	Write	user*		
UploadServerCertificate	Gewährt die Berechtigung zum Hochladen einer Serverzertifikat-Entity für das AWS-Konto	Write	server-certificate*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UploadSigningCertificate	Gewährt die Berechtigung zum Upload eines X.509-Signaturzertifikats und zum Zuordnen des Zertifikats zum angegebenen IAM-Benutzer.	Schreiben	user*		

Von AWS Identity and Access Management (IAM) definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
access-report	`arn:${Partition}:iam::${Account}:access-report/${EntityPath}`	
assumed-role	`arn:${Partition}:iam::${Account}:assumed-role/${RoleName}/${RoleSessionName}`	
federated-user	`arn:${Partition}:iam::${Account}:federated-user/${UserName}`	
group	`arn:${Partition}:iam::${Account}:group/${GroupNameWithPath}`	
instance-profile	`arn:${Partition}:iam::${Account}:instance-profile/${InstanceProfileNameWithPath}`	aws:ResourceTag/${TagKey}
mfa	`arn:${Partition}:iam::${Account}:mfa/${MfaTokenIdWithPath}`	aws:ResourceTag/${TagKey}
oidc-provider	`arn:${Partition}:iam::${Account}:oidc-provider/${OidcProviderName}`	aws:ResourceTag/${TagKey}
policy	`arn:${Partition}:iam::${Account}:policy/${PolicyNameWithPath}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
role	`arn:${Partition}:iam::${Account}:role/${RoleNameWithPath}`	aws:ResourceTag/${TagKey} iam:ResourceTag/${TagKey}
saml-provider	`arn:${Partition}:iam::${Account}:saml-provider/${SamlProviderName}`	aws:ResourceTag/${TagKey}
server-certificate	`arn:${Partition}:iam::${Account}:server-certificate/${CertificateNameWithPath}`	aws:ResourceTag/${TagKey}
sms-mfa	`arn:${Partition}:iam::${Account}:sms-mfa/${MfaTokenIdWithPath}`	
user	`arn:${Partition}:iam::${Account}:user/${UserNameWithPath}`	aws:ResourceTag/${TagKey} iam:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Identity and Access Management (IAM)

AWS Identity and Access Management (IAM) definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüsseln, die in der Anforderung übergeben werden.	ArrayOfString
iam:AWSServiceName	Filtert den Zugriff anhand des AWS-Service, dem diese Rolle angefügt ist	Zeichenfolge
iam:AssociatedResourceArn	Filtert den Zugriff nach der Ressource, in deren Auftrag die Rolle verwendet wird	ARN
iam:FIDO-FIPS-140-2-certification	Filtert den Zugriff nach der FIPS-140-2-Validierungsstufe des MFA-Geräts zum Zeitpunkt der Registrierung eines FIDO-Sicherheitsschlüssels	Zeichenfolge
iam:FIDO-FIPS-140-3-certification	Filtert den Zugriff nach der FIPS-140-3-Validierungsstufe des MFA-Geräts zum Zeitpunkt der Registrierung eines FIDO-Sicherheitsschlüssels	Zeichenfolge
iam:FIDO-certification	Filtert den Zugriff nach der FIDO-Zertifizierungsstufe des MFA-Geräts zum Zeitpunkt der Registrierung eines FIDO-Sicherheitsschlüssels	Zeichenfolge
iam:OrganizationsPolicyId	Filtert den Zugriff anhand der ID einer AWS-Organizations-Richtlinie	Zeichenfolge
iam:PassedToService	Filtert den Zugriff anhand des AWS-Service, dem diese Rolle übergeben wird	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
iam:PermissionsBoundary	Filtert den Zugriff, wenn die angegebene Richtlinie für die IAM-Entity (Benutzer oder Rolle) als Berechtigungsgrenze festgelegt ist.	ARN
iam:PolicyARN	Filtert den Zugriff anhand des ARNs einer IAM-Richtlinie.	ARN
iam:RegisterSecurityKey	Filtert den Zugriff nach dem aktuellen Status der MFA-Geräteaktivierung	Zeichenfolge
iam:ResourceTag/${TagKey}	Filtert den Zugriff anhand der Tags, die einer IAM-Entity (Benutzer oder Rolle) angefügt sind.	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Identity And Access Management

AWS Identity and Access Management Roles Anywhere (Dienstpräfix:`rolesanywhere`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Identity And Access Management definierte Aktionen
- Von AWS Identity and Access Management definierte Ressourcentypen
- Bedingungsschlüssel für AWS Identity And Access Management

Von AWS Identity And Access Management definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateProfile	Gewährt die Berechtigung zum Erstellen einer Profilaufgabe	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
CreateTrustAnchor	Gewährt die Berechtigung zum Erstellen eines Trust Anchors	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAttributeMapping	Erteilt die Berechtigung zum Löschen einer Zuordnungsregel aus einem Profil	Schreiben	profile*		
DeleteCrl	Gewährt die Berechtigung zum Löschen einer Zertifikatswiderrufsliste (CRL)	Schreiben	crl*		
DeleteProfile	Gewährt die Berechtigung zum Löschen eines Profils	Schreiben	profile*		
DeleteTrustAnchor	Gewährt die Berechtigung zum Löschen eines Trust Anchors	Schreiben	trust-anchor*		
DisableCrl	Gewährt die Berechtigung zum Deaktivieren einer Zertifikatswiderrufsliste (CRL)	Schreiben	crl*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisableProfile	Gewährt die Berechtigung zum Ändern einer Profilaufgabe	Schreiben	profile*		
DisableTrustAnchor	Gewährt die Berechtigung zum Deaktivieren eines Trust Anchors	Schreiben	trust-anchor*		
EnableCrl	Gewährt die Berechtigung zum Aktivieren einer Zertifikatswiderrufsliste (CRL)	Schreiben	crl*		
EnableProfile	Gewährt die Berechtigung zum Löschen eines Profils	Schreiben	profile*		iam:PassRole
EnableTrustAnchor	Gewährt die Berechtigung zum Aktivieren eines Trust Anchors	Schreiben	trust-anchor*		
GetCrl	Gewährt die Berechtigung zum Abrufen einer Zertifikatswiderrufsliste (CRL)	Lesen	crl*		
GetProfile	Gewährt die Berechtigung zum Abrufen eines Startprofils	Lesen	profile*		
GetSubject	Gewährt die Berechtigung zum Abrufen einer Suite-Ausführung	Lesen	subject*		
GetTrustAnchor	Gewährt die Berechtigung zum Erhalten eines Trust Anchors	Lesen	trust-anchor*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ImportCrl	Gewährt die Berechtigung zum Importieren einer Zertifikatswiderrufsliste (CRL)	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
ListCrls	Erteilt die Berechtigung zum Auflisten von Zertifikatssperrlisten (CRLs)	Auflisten			
ListProfiles	Gewährt die Berechtigung zum Auflisten von Startprofilen	Auflisten			
ListSubjects	Gewährt die Berechtigung, Themen aufzulisten	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Auflisten			
ListTrustAnchors	Gewährt die Berechtigung zum Auflisten eines Trust Anchors	Auflisten			
PutAttributeMapping	Erteilt die Berechtigung, eine Zuordnungsregel in ein Profil einzufügen	Schreiben	profile*		
PutNotificationSettings	Gewährt die Berechtigung zum Anhängen von Benachrichtigungseinstellungen an einen Trust Anchor	Schreiben	trust-anchor*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ResetNotificationSettings	Gewährt die Berechtigung, benutzerdefinierte Benachrichtigungseinstellungen auf den von IAM Roles Anywhere definierten Standardstatus zurückzusetzen	Schreiben	trust-anchor*		
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren	crl		
			profile		
			subject		
			trust-anchor		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Tagging	crl		
			profile		
			subject		
			trust-anchor		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateCrl	Gewährt die Berechtigung zum Aktualisieren einer Zertifikatswiderrufsliste (CRL)	Schreiben	crl*		
UpdateProfile	Gewährt die Berechtigung zum Aktualisieren eines Startprofils	Schreiben	profile*		iam:PassRole
UpdateTrustAnchor	Gewährt die Berechtigung zum Aktualisieren eines Trust Anchors	Schreiben	trust-anchor*		

Von AWS Identity and Access Management definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
trust-anchor	`arn:${Partition}:rolesanywhere:${Region}:${Account}:trust-anchor/${TrustAnchorId}`	aws:ResourceTag/${TagKey}
profile	`arn:${Partition}:rolesanywhere:${Region}:${Account}:profile/${ProfileId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
subject	`arn:${Partition}:rolesanywhere:${Region}:${Account}:subject/${SubjectId}`	aws:ResourceTag/${TagKey}
crl	`arn:${Partition}:rolesanywhere:${Region}:${Account}:crl/${CrlId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Identity And Access Management

AWS Identity and Access Management Roles Anywhere definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Identity Store

AWS Identity Store (Service-Präfix: `identitystore`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Identity Store definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateGroup	Gewährt die Berechtigung zum Erstellen einer Gruppe im angegebenen IdentityStore	Schreiben	Identitystore*		
CreateGroupMembership	Erteilt die Berechtigung zum Erstellen eines Mitglieds für eine Gruppe im angegebenen IdentityStore	Schreiben	Group*		
			Identitystore*		
			User*		
CreateUser	Erteilt die Berechtigung zum Erstellen eines Benutzers im angegebenen IdentityStore	Schreiben	Identitystore*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteGroup	Gewährt die Berechtigung zum Löschen einer Gruppe im angegebenen IdentityStore	Schreiben	Group*		
			Identitystore*		
DeleteGroupMembership	Erteilt die Berechtigung zum Entfernen eines Mitglieds, das Teil einer Gruppe im angegebenen IdentityStore ist	Schreiben	Group*		
			GroupMembership*		
			Identitystore*		
			User*		
DeleteUser	Erteilt die Berechtigung zum Löschen eines Benutzers im angegebenen IdentityStore	Schreiben	Identitystore*		
			User*		
DescribeGroup	Erteilt die Berechtigung zum Abrufen von Informationen über eine Gruppe im angegebenen IdentityStore	Lesen	Group*		
			Identitystore*		
DescribeGroupMembership	Erteilt die Berechtigung zum Abrufen von Informationen über ein Mitglied, das Teil einer Gruppe im angegebenen IdentityStore ist	Lesen	Group*		
			GroupMembership*		
			Identitystore*		
			User*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeUser	Erteilt die Berechtigung zum Abrufen von Informationen über den Benutzer im angegebenen IdentityStore	Lesen	Identitystore*		
			User*		
GetGroupId	Erteilt die Berechtigung zum Abrufen von ID-Informationen zur Gruppe im angegebenen IdentityStore	Lesen	Group*		
			Identitystore*		
GetGroupMembershipId	Erteilt die Berechtigung zum Abrufen von ID-Informationen eines Mitglieds, das Teil einer Gruppe im angegebenen IdentityStore ist	Lesen	Group*		
			GroupMembership*		
			Identitystore*		
			User*		
GetUserId	Erteilt die Berechtigung zum Abrufen von ID-Informationen über den Benutzer im angegebenen IdentityStore	Lesen	Identitystore*		
			User*		
IsMemberInGroups	Erteilt die Berechtigung zum Überprüfen, ob ein Mitglied Teil von Gruppen im angegebenen IdentityStore ist	Lesen	AllGroupMemberships*		
			Group*		
			Identitystore*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			User*		
ListGroupMemberships	Erteilt die Berechtigung zum Abrufen aller Mitglieder, die Teil einer Gruppe im angegebenen IdentityStore sind	Auflisten	AllGroupMemberships*		
			Group*		
			Identitystore*		
ListGroupMembershipsForMember	Erteilt die Berechtigung, Gruppen des Zielelements im angegebenen IdentityStore aufzulisten	Auflisten	AllGroupMemberships*		
			Identitystore*		
			User*		
ListGroups	Erteilt die Berechtigung zum Suchen nach Gruppen innerhalb des angegebenen IdentityStore	Auflisten	AllGroups*		
			Identitystore*		
ListUsers	Erteilt die Berechtigung zum Suchen nach Benutzern im angegebenen IdentityStore	Auflisten	AllUsers*		
			Identitystore*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateGroup	Erteilt die Berechtigung zum Aktualisieren von Informationen über eine Gruppe im angegebenen IdentityStore	Schreiben	Group*		
			Identitystore*		
UpdateUser	Erteilt die Berechtigung zum Aktualisieren von Benutzerinformationen im angegebenen IdentityStore	Schreiben	Identitystore*		
			User*		

Vom AWS Identity Store definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Identitystore	`arn:${Partition}:identitystore::${Account}:identitystore/${IdentityStoreId}`	
User	`arn:${Partition}:identitystore:::user/${UserId}`	
Group	`arn:${Partition}:identitystore:::group/${GroupId}`	

Ressourcentypen	ARN	Bedingungsschlüssel
GroupMembership	`arn:${Partition}:identitystore:::membership/${MembershipId}`	
AllUsers	`arn:${Partition}:identitystore:::user/*`	
AllGroups	`arn:${Partition}:identitystore:::group/*`	
AllGroupMemberships	`arn:${Partition}:identitystore:::membership/*`	

Bedingungsschlüssel für AWS Identity Store

AWS Identity Store definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
identitystore:UserId	Filtert den Zugriff nach der IAM-Identity-Center-Benutzer-ID	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel Identitätsspeicher-Authentifizierung für AWS

Die Identitätsspeicher-Authentifizierung für AWS (Service-Präfix: `identitystore-auth`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von der Identitätsspeicher-Authentifizierung für AWS definierte Aktionen
- Vom der Identitätsspeicher-Authentifizierung für AWS definierte Ressourcentypen
- Bedingungsschlüssel für die Identitätsspeicher-Authentifizierung für AWS

Von der Identitätsspeicher-Authentifizierung für AWS definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchDeleteSession [nur Berechtigung]	Gewährt die Berechtigung zum Löschen eines Batch von angegebenen Sitzungen	Schreiben			
BatchGetSession [nur Berechtigung]	Gewährt die Berechtigung, Sitzungsattribute für einen Batch angegebener Sitzungen zurückzugeben	Lesen			
ListSessions [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen einer Liste der aktiven Sitzungen für den angegebenen Benutzer	Auflisten			

Vom der Identitätsspeicher-Authentifizierung für AWS definierte Ressourcentypen

Die Identitätsspeicher-Authentifizierung für AWS unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf die Identitätsspeicher-Authentifizierung für AWS zu ermöglichen, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für die Identitätsspeicher-Authentifizierung für AWS

Die Identitätsspeicher-Authentifizierung besitzt keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS die Identitätssynchronisierung

AWS Identity Sync (Servicepräfix: `identity-sync`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Durch die AWS Identitätssynchronisation definierte Aktionen
- Von AWS Identitätssynchronisation definierte Ressourcentypen
- Bedingungsschlüssel für AWS Identitätssynchronisation

Durch die AWS Identitätssynchronisation definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWSzu erteilen.

Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AllowVendedLogDeliveryForResource [nur Berechtigung]	Gewährt die Berechtigung zum Konfigurieren der Bereitstellung von Vended-Protokollen für ein Sync-Profil	Berechtigungsverwaltung	SyncProfileResource*		
CreateSyncFilter	Gewährt die Berechtigung zum Erstellen eines Synchronisierungsfilters im Synchronisierungsprofil	Schreiben	SyncProfileResource*		
CreateSyncProfile	Erteilung der Berechtigung zur Erstellung eines Synchronisationsprofils für die Identitätsquelle	Schreiben			ds:AuthorizeApplication
CreateSyncTarget	Erteilung der Berechtigung zum Erstellen eines Synchronisierungsziels für die Identitätsquelle	Schreiben	SyncProfileResource*		
DeleteSyncFilter	Erteilung der Berechtigung zum Löschen eines Synchronisationsfilters aus dem Synchronisationsprofil	Schreiben	SyncProfileResource*		
DeleteSyncProfile	Erteilung der Berechtigung zum Löschen eines Synchronisationsprofils aus der Quelle	Schreiben	SyncProfileResource*		ds:UnauthorizeApplication
DeleteSyncTarget	Erteilung der Berechtigung zum Löschen eines Synchronisationsziels aus der Quelle	Schreiben	SyncProfileResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			SyncTargetResource*		
GetSyncProfile	Erteilung der Berechtigung zum Abrufen eines Synchronisationsprofils unter Verwendung eines Synchronisationsprofilnamens	Lesen	SyncProfileResource*		
GetSyncTarget	Erteilung der Berechtigung zum Abrufen eines Synchronisierungsziels aus dem Synchronisierungsprofil	Lesen	SyncProfileResource*		
			SyncTargetResource*		
ListSyncFilters	Ermöglicht die Auflistung der Synchronisierungsfilter aus dem Synchronisierungsprofil	Auflisten	SyncProfileResource*		
StartSync	Erteilung der Berechtigung zum Starten eines Synchronisierungsvorgangs oder zur Wiederaufnahme eines zuvor angehaltenen Synchronisierungsvorgangs	Schreiben	SyncProfileResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopSync	Erteilung der Berechtigung, den Start eines geplanten Synchronisierungsvorgangs im Synchronisierungsplan zu stoppen	Schreiben	SyncProfileResource*		
UpdateSyncTarget	Gewährt die Berechtigung zum Aktualisieren eines Synchronisierungsziels im Synchronisierungsprofil	Schreiben	SyncProfileResource*		
			SyncTargetResource*		

Von AWS Identitätssynchronisation definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
SyncProfileResource	`arn:${Partition}:identity-sync:${Region}:${Account}:profile/${SyncProfileName}`	

Ressourcentypen	ARN	Bedingungsschlüssel
SyncTargetResource	`arn:${Partition}:identity-sync:${Region}:${Account}:target/${SyncProfileName}/${SyncTargetName}`	

Bedingungsschlüssel für AWS Identitätssynchronisation

Identitätssynchronisation hat keine servicespezifischen Kontextschlüssel, die in den `Condition` Elementen von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Import Export Disk Service

AWS Import Export Disk Service (Servicepräfix: `importexport`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Import Export Disk Service definierte Aktionen
- Von AWS Import Export Disk Service definierte Ressourcentypen
- Bedingungsschlüssel für AWS Import Export Disk Service

Von AWS Import Export Disk Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelJob	Mit dieser Aktion wird ein bestimmter Auftrag storniert. Die Stornierung ist auf den Auftragseigentümer beschränkt. Wenn der Auftrag bereits begonnen oder abgeschlossen wurde, kann die Aktion nicht ausgeführt werden.	Write			
CreateJob	Diese Aktion initiiert den Planungsprozess für einen Upload oder Download Ihrer Daten.	Write			
GetShippingLabel	Mit dieser Aktion wird ein vorfrankiertes Versandetikett generiert, mit dem Sie Ihr Gerät zur Verarbeitung an AWS senden.	Read			
GetStatus	Diese Aktion gibt Informationen über einen Auftrag zurück, darunter die Position des Auftrags in der Verarbeitungspipeline, den Status der Ergebnisse und den Signaturwert, der dem Auftrag zugeordnet ist.	Read			
ListJobs	Diese Aktion gibt die Aufträge zurück, die dem Auftraggeber zugeordnet sind.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateJob	Verwenden Sie die Aktion, um die in der ursprünglichen Manifestdatei angegeben Parameter zu ändern, indem Sie eine neue Manifestdatei bereitstellen.	Write			

Von AWS Import Export Disk Service definierte Ressourcentypen

AWS Import Export Disk Service unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf den AWS Import Export Disk Service zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Import Export Disk Service

Import/Export besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Inspector

Amazon Inspector (Servicepräfix: `inspector`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Inspector definierte Aktionen
- Von Amazon Inspector definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Inspector

Von Amazon Inspector definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddAttributesToFindings	Gewährt die Berechtigung zum Zuweisen von Attributen (Schlüssel/Wert-Paare) zu den Ergebnissen, die von den ARNs der Ergebnisse angegebenen werden	Write			
CreateAssessmentTarget	Gewährt die Berechtigung, ein neues Bewertungsziel mit dem ARN der Ressourcengruppe zu erstellen, die von CreateResourceGroup generiert wird	Write			
CreateAssessmentTemplate	Gewährt die Berechtigung, eine Bewertungsvorlage für das über seinen ARN angegebene Bewertungsziel zu erstellen	Write			
CreateExclusionsPreview	Gewährt die Berechtigung zum Starten der Erstellung einer Ausschlussvorschau für die angegebene Bewertungsvorlage	Write			
CreateResourceGroup	Gewährt die Berechtigung, eine Ressourcengruppe unter Verwendung des angegebenen Satzes von Tags (Schlüssel/Wert-Paare) zu erstellen	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	, die zur Auswahl der in ein Amazon-Inspector-Bewertungsziel einzuschließenden EC2-Instances verwendet werden				
DeleteAssessmentRun	Gewährt die Berechtigung zum Löschen des Bewertungslaufs, der durch den ARN des Bewertungslaufs festgelegt ist	Write			
DeleteAssessmentTarget	Gewährt die Erlaubnis, das Bewertungsziel zu löschen, das durch den ARN des Bewertungsziels festgelegt ist	Write			
DeleteAssessmentTemplate	Gewährt die Berechtigung, die über ihren ARN angegebene Bewertungsvorlage zu löschen	Write			
DescribeAssessmentRuns	Gewährt die Erlaubnis zur Beschreibung der Bewertungsläufe, die durch die ARNs der Bewertungsläufe festgelegt werden	Read			
DescribeAssessmentTargets	Gewährt die Berechtigung zur Beschreibung der Bewertungsziele, die von den ARNs der Bewertungsziele festgelegt werden	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeAssessmentTemplates	Gewährt die Berechtigung zum Beschreiben der Bewertungsvorlagen, die von den ARNs der Bewertungsvorlagen angegeben werden	Read			
DescribeCrossAccountAccessRole	Gewährt die Berechtigung zur Beschreibung der IAM-Rolle, die Amazon Inspector den Zugriff auf Ihr AWS-Konto ermöglicht	Read			
DescribeExclusions	Gewährt die Erlaubnis, die Ausschlüsse zu beschreiben, die durch die ARNs der Ausschlüsse festgelegt werden	Read			
DescribeFindings	Gewährt die Erlaubnis, die Ergebnisse zu beschreiben, die von den ARNs der Ergebnisse angegeben werden	Read			
DescribeResourceGroups	Gewährt die Berechtigung zur Beschreibung der Resource Groups, die von den ARNs der Resource Groups angegeben werden	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeRulesPackages	Gewährt die Berechtigung zur Beschreibung der Regelpakete, die von den ARNs der Regelpakete angegeben werden	Read			
GetAssessmentReport	Gewährt die Erlaubnis zur Erstellung eines Bewertungsberichts, der detaillierte und umfassende Ergebnisse eines bestimmten Bewertungslaufs enthält	Read			
GetExclusionsPreview	Gewährt die Berechtigung zum Abrufen der Ausschlussvorschau (eine Liste von ExclusionPreview-Objekten), die durch das Vorschau-Token angegeben wird	Read			
GetTelemetryMetadata	Gewährt die Berechtigung, Informationen zu den Daten zu erhalten, die für den angegebenen Bewertungslauf erfasst werden	Read			
ListAssessmentRunAgents	Gewährt die Berechtigung, die Agenten der über ihre ARNs angegebenen Bewertungsläufe aufzulisten	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAssessmentRuns	Gewährt die Berechtigung, die Bewertungsläufe aufzulisten, die den über ihre ARNs angegebenen Bewertungsvorlagen entsprechen	List			
ListAssessmentTargets	Gewährt die Erlaubnis, die ARNs der Bewertungsziele in diesem AWS-Konto aufzulisten	List			
ListAssessmentTemplates	Gewährt die Berechtigung, die Bewertungsvorlagen aufzulisten, die den über ihre ARNs angegebenen Bewertungszielen entsprechen	List			
ListEventSubscriptions	Gewährt die Berechtigung, alle Ereignisabonnements für die über ihren ARN angegebene Bewertungsvorlage aufzulisten	List			
ListExclusions	Gewährt die Berechtigung zum Auflisten von Ausschlüssen, die durch den Bewertungslauf generiert werden	List			
ListFindings	Gewährt die Berechtigung, die Ergebnisse aufzulisten, die von den über ihre ARNs angegebenen Bewertungsläufen generiert werden	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListRulesPackages	Gewährt die Berechtigung zum Auflisten aller verfügbaren Amazon-Inspector-Regelpakete	List			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten aller mit einer Bewertungsvorlage verknüpften Tags	Read			
PreviewAgents	Gewährt die Berechtigung zur Vorschau der auf den EC2-Instances installierten Agenten, die Teil des angegebenen Bewertungsziels sind	Read			
RegisterCrossAccountAccessRole	Gewährt die Berechtigung, die IAM-Rolle zu registrieren, die Amazon Inspector verwendet, um EC2-Instances zu Beginn des Bewertungslaufs oder beim Aufrufen der Aktion PreviewAgents aufzulisten	Write			
RemoveAttributesFromFindings	Gewährt die Berechtigung, alle Attribute (Schlüssel/Wert-Paare) aus den über ihre ARNs angegebenen Ergebnissen zu entfernen, die ein Attribut mit dem angegebenen Schlüssel enthalten	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SetTagsForResource	Gewährt die Berechtigung, Tags (Schlüssel/Wert-Paare) für die über ihren ARN angegebene Bewertungsvorlage festzulegen	Markieren			
StartAssessmentRun	Gewährt die Erlaubnis, den im ARN der Bewertungsvorlage festgelegten Bewertungslauf zu starten	Write			
StopAssessmentRun	Gewährt die Berechtigung zum Stoppen des Bewertungslaufs, der durch den ARN des Bewertungslaufs festgelegt ist	Write			
SubscribeToEvent	Gewährt die Berechtigung, das Verfahren zum Senden von Amazon-Simple-Notification-Service(SNS)-Benachrichtigungen zu einem angegebenen Ereignis an ein angegebenes SNS-Thema zu aktivieren	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UnsubscribeFromEvent	Gewährt die Berechtigung, das Verfahren zum Senden von Amazon-Simple-Notification-Service(SNS)-Benachrichtigungen zu einem angegebenen Ereignis an ein angegebenes SNS-Thema zu deaktivieren	Write			
UpdateAssessmentTarget	Gewährt die Erlaubnis zur Aktualisierung des Bewertungsziels, das durch den ARN des Bewertungsziels festgelegt ist	Write			

Von Amazon Inspector definierte Ressourcentypen

Amazon Inspector unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf Amazon Inspector zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für Amazon Inspector

Inspector besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Inspector2

Amazon Inspector2 (Servicepräfix: `inspector2`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Inspector2 definierte Aktionen
- Von Amazon Inspector2 definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Inspector2

Von Amazon Inspector2 definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateMember	Gewährt die Berechtigung, ein Konto einem Amazon-Inspector-Administratorkonto zuzuordnen	Schreiben			
BatchGetAccountStatus	Gewährt die Berechtigung zum Abrufen von Informationen über Amazon–Inspector-Konten für ein Konto	Lesen			
BatchGetCodeSnippet	Gewährt die Berechtigung zum Abrufen von Code-Snippet-Informationen zu einem oder mehreren Code-Schwachstellen-Ergebnissen	Lesen			
BatchGetFindingDetails	Erteilt die Berechtigung, einem Kunden bei Auffinden einer Schwachstelle zusätzliche Informationen bereitzustellen	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetFreeTrialInfo	Gewährt die Berechtigung zum Abrufen der Berechtigung zum kostenlosen Testzeitraum für Amazon-Inspector-Konten für ein Konto	Lesen			
BatchGetMemberEc2DeepInspectionStatus	Gewährt dem delegierten Administrator die Berechtigung, den ec2 Deep-Inspection-Status von Mitgliedskonten abzurufen	Lesen			
BatchUpdateMemberEc2DeepInspectionStatus	Gewährt die Berechtigung zur Aktualisierung des Status der ec2 Deep-Inspection durch den delegierten Administrator für seine zugehörigen Mitgliedskonten	Schreiben			
CancelFindingsReport	Gewährt die Berechtigung zum Aufheben der Erstellung eines Ergebnisberichts	Schreiben			
CancelSbomExport	Gewährt die Berechtigung zum Aufheben der Erstellung eines SBOM-Berichts	Schreiben			
CreateCisScanConfiguration	Gewährt die Berechtigung zum Erstellen und Definieren der Einstellungen für eine CIS-Scan-Konfiguration	Schreiben	CIS Scan Configuration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateFilter	Gewährt die Berechtigung zum Erstellen und Definieren der Einstellungen für einen Ergebnisfilter.	Schreiben	Filter*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFindingsReport	Gewährt die Berechtigung, die Erstellung eines Ergebnisberichts anzufordern	Schreiben			
CreateSbomExport	Gewährt die Berechtigung zum Anfordern der Erstellung eines SBOM-Berichts	Schreiben			
DeleteCisScanConfiguration	Gewährt die Berechtigung zum Löschen einer CIS-Scankonfiguration	Schreiben	CIS Scan Configuration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
DeleteFilter	Gewährt die Berechtigung zum Löschen eines Ergebnisfilters.	Schreiben	Filter*		
DescribeOrganizationConfiguration	Gewährt die Berechtigung zum Abrufen von Informationen zu den Amazon-Inspector-Konfigurationseinstellungen für eine AWS-Organisation	Lesen			
Disable	Gewährt die Berechtigung zum Deaktivieren eines Amazon-Inspector-Kontos	Schreiben			
DisableDelegatedAdminAccount	Gewährt die Berechtigung zum Deaktivieren eines Kontos als delegiertes Amazon-Inspector-Administratorkonto für eine AWS-Organisation	Schreiben			
DisassociateMember	Gewährt einem Amazon-Inspector-Administratorkonto die Berechtigung, die Verknüpfung mit einem Inspector-Mitgliedskonto aufzuheben	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Enable	Gewährt die Berechtigung zum Aktivieren und Festlegen der Konfigurationseinstellungen für ein neues Amazon-Inspector-Konto	Schreiben			
EnableDelegatedAdminAccount	Gewährt die Berechtigung zum Aktivieren eines Kontos als delegiertes Amazon-Inspector-Administratorkonto für eine AWS-Organisation	Schreiben			
GetCisScanReport	Gewährt die Berechtigung zum Abrufen eines Berichts, der Informationen zu abgeschlossenen CIS-Scans enthält	Lesen			
GetCisScanResultDetails	Gewährt die Berechtigung zum Abrufen von Informationen zu allen Details zu einem CIS-Scan und einer Zielressource	Auflisten			
GetConfiguration	Erteilt die Berechtigung zum Abrufen von Informationen zu den Amazon-Inspector-Konfigurationseinstellungen für ein AWS-Konto	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDelegatedAdminAccount	Gewährt die Berechtigung zum Abrufen von Informationen über das Amazon-Inspector-Administratorkonto für ein Konto	Lesen			
GetEc2DeepInspectionConfiguration	Gewährt die Berechtigung zum Abruf der ec2-Deep-Inspection-Konfiguration für eigenständige Konten, delegierte Administratoren und Mitgliedskonten	Lesen			
GetEncryptionKey	Gewährt die Berechtigung zum Abrufen von Informationen zum KMS-Schlüssel zum Verschlüsseln von Codefragmenten	Lesen			
GetFindingsReportStatus	Gewährt die Berechtigung zum Abrufen des Status für einen angeforderten Ergebnisbericht	Lesen			
GetMember	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Konto abzurufen, das einem Amazon-Inspector-Administratorkonto zugeordnet ist	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetSbomExport	Gewährt die Berechtigung zum Abrufen eines angeforderten SBOM-Berichts	Lesen			
ListAccountPermissions	Gewährt die Berechtigung zum Abrufen der Konfigurations-Berechtigungen für Funktionen, die einem Amazon-Inspector-Konto innerhalb einer Organisation zugeordnet sind	Auflisten			
ListCisScanConfigurations	Gewährt die Berechtigung zum Abrufen von Informationen zu allen CIS-Scankonfigurationen	Auflisten			
ListCisScanResultsAggregatedByChecks	Gewährt die Berechtigung zum Abrufen von Informationen zu allen Prüfungen, die sich auf einen CIS-Scan beziehen	Auflisten			
ListCisScanResultsAggregatedByTargetResource	Gewährt die Berechtigung zum Abrufen von Informationen zu allen Ressourcen, die sich auf einen CIS-Scan beziehen	Auflisten			
ListCisScans	Gewährt die Berechtigung zum Abrufen von Informationen zu abgeschlossenen CIS-Scans	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListCoverage	Gewährt die Berechtigung zum Abrufen der Arten von Statistiken, die Amazon Inspector für Ressourcen generieren kann, die Inspector überwacht	Auflisten			
ListCoverageStatistics	Gewährt die Berechtigung zum Abrufen statistischer Daten und anderer Informationen über die Ressourcen, die Amazon Inspector überwacht	Auflisten			
ListDelegatedAdminAccounts	Gewährt die Berechtigung zum Abrufen von Informationen über das delegierte Amazon-Inspector-Administratorkonto für eine AWS-Organisation	Auflisten			
ListFilters	Gewährt die Berechtigung zum Abrufen von Informationen über alle Ergebnisfilter	Auflisten			
ListFindingAggregations	Gewährt die Berechtigung zum Abrufen statistischer Daten und anderer Informationen zu den Ergebnissen von Amazon Inspector	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListFindings	Gewährt die Berechtigung zum Abrufen einer Teilmenge von Informationen zu einem oder mehreren Ergebnissen.	Auflisten			
ListMembers	Gewährt die Berechtigung zum Abrufen von Informationen über Amazon-Inspector-Mitgliedskonten, die einem Amazon-Inspector-Administrator-Konto zugeordnet sind	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Abrufen der Tags für eine Amazon-Inspector-Ressource	Lesen			
ListUsageTotals	Gewährt die Berechtigung zum Abrufen aggregierter Nutzungsdaten für ein Konto.	Auflisten			
ResetEncryptionKey	Gewährt die Berechtigung, einem Kunden die Möglichkeit zu geben, einen Amazon-eigenen KMS-Schlüssel zum Verschlüsseln von Codefragmenten zu verwenden	Schreiben			
SearchVulnerabilities	Gewährt die Berechtigung zur Auflistung der Abdeckungsdetails von Amazon Inspector für eine bestimmte Schwachstelle	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SendCisSessionHealth	Gewährt die Berechtigung zum Senden des CIS-Zustands für einen CIS-Scan	Schreiben			
SendCisSessionTelemetry	Gewährt die Berechtigung zum Senden von CIS-Telemetrie für einen CIS-Scan	Schreiben			
StartCisSession	Gewährt die Berechtigung zum Starten einer CIS-Scansitzung	Schreiben			
StopCisSession	Gewährt die Berechtigung zum Beenden einer CIS-Scansitzung	Schreiben			
TagResource	Gewährt die Berechtigung zum Hinzufügen oder Aktualisieren der Tags für eine Amazon-Inspector-Ressource	Tagging	CIS Scan Configuration	inspector2:CisScanConfiguration	
			Filter	inspector2:Filter	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Amazon-Inspector-Ressource	Tagging	CIS Scan Configuration	inspector2:CisScanConfiguration	
			Filter	inspector2:Filter	
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCisScanConfiguration	Gewährt die Berechtigung zum Aktualisieren der Einstellungen für eine CIS-Scan-Konfiguration	Schreiben	CIS Scan Configuration*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateConfiguration	Erteilt die Berechtigung zum Aktualisieren von Informationen zu den Amazon-Inspector-Konfigurationseinstellungen für ein AWS-Konto	Schreiben			
UpdateEc2DeepInspectionConfiguration	Gewährt die Berechtigung zur Aktualisierung der ec2-Deep-Inspection-Konfiguration durch delegierte Administratoren, Mitglieder und eigenständige Konten	Schreiben			
UpdateEncryptionKey	Gewährt die Berechtigung, einem Kunden die Möglichkeit zu geben, einen KMS-Schlüssel zum Verschlüsseln von Codeausschnitten zu verwenden	Schreiben			
UpdateFilter	Gewährt die Berechtigung zum Aktualisieren der Einstellungen für einen Ergebnisfilter.	Schreiben	Filter*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateOrgEc2DeepInspectionConfiguration	Gewährt die Berechtigung zur Aktualisierung der ec2-Deep-Inspection-Konfiguration durch den delegierten Administrator für seine zugehörigen Mitgliedskonten	Schreiben			
UpdateOrganizationConfiguration	Gewährt die Berechtigung zum Aktualisieren der Amazon–Inspector-Konfigurationseinstellungen für eine AWS-Organisation	Schreiben			

Von Amazon Inspector2 definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Filter	`arn:${Partition}:inspector2:${Region}:${Account}:owner/${OwnerId}/filter/${FilterId}`	aws:ResourceTag/${TagKey}
Finding	`arn:${Partition}:inspector2:${Region}:${Account}:finding/${FindingId}`	

Ressourcentypen	ARN	Bedingungsschlüssel
CIS Scan Configuration	`arn:${Partition}:inspector2:${Region}:${Account}:owner/${OwnerId}/cis-configuration/${CISScanConfigurationId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Inspector2

Amazon Inspector2 definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	String
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon InspectorScan

Amazon InspectorScan (Service-Präfix: `inspector-scan`) bietet die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon InspectorScan definierte Aktionen
- Von Amazon InspectorScan definierte Ressourcentypen
- Bedingungsschlüssel für Amazon InspectorScan

Von Amazon InspectorScan definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ScanSbom	Gewährt die Berechtigung, die vom Kunden bereitgestellte SBOM zu scannen und die darin gefundenen Schwachstellen zurückzugeben	Lesen			

Von Amazon InspectorScan definierte Ressourcentypen

Amazon InspectorScan unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf Amazon InspectorScan zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für Amazon InspectorScan

InspectorScan besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Interactive Video Service

Amazon Interactive Video Service (Servicepräfix: `ivs`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Interactive Video Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetChannel	Gewährt die Berechtigung, mehrere Kanäle gleichzeitig nach Kanal-ARN zu erhalten.	Read	Channel*		
BatchGetStreamKey	Gewährt die Berechtigung, mehrere Stream-Schlüssel gleichzeitig nach Stream-Schlüssel-ARN zu erhalten.	Lesen	Stream-Key*		
BatchStartViewerSessionRevocation	Gewährt die Berechtigung zum gleichzeitigen Ausführen StartViewerSessionRevocatio	Schreiben	Channel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	n von für mehrere Kanal-ARN- und Viewer-ID-Paare				
CreateChannel	Gewährt die Berechtigung zum Erstellen eines neuen Kanals und eines zugeordneten Stream-Schlüssels.	Schreiben	Channel*		
			Stream-Key*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEncoderConfiguration	Gewährt die Berechtigung zum Erstellen einer neuen Encoder-Konfiguration	Schreiben	Encoder-Configuration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateParticipantToken	Gewährt die Berechtigung zum Erstellen eines Teilnehmer-Tokens	Schreiben	Stage*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreatePlaybackRestrictionPolicy	Gewährt die Berechtigung zum Erstellen einer Wiedergabe-Einschränkungsrichtlinie	Schreiben	Playback-Restriction-Policy*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRecordingConfiguration	Gewährt die Berechtigung zum Erstellen einer neuen Aufzeichnungskonfiguration	Schreiben	Recording-Configuration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStage	Gewährt die Berechtigung zum Erstellen einer Stufe	Schreiben	Stage*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateStorageConfiguration	Gewährt die Berechtigung zum Erstellen einer neuen Speicherkonfiguration	Schreiben	Storage-Configuration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStreamKey	Gewährt die Berechtigung zum Erstellen eines Stream-Schlüssels.	Write	Stream-Key*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteChannel	Gewährt die Berechtigung zum Löschen eines Kanals und der Stream-Schlüssel des Kanals.	Schreiben	Channel*		
			Stream-Key*		
DeleteEncoderConfiguration	Gewährt die Berechtigung zum Löschen einer Encoder-Konfiguration q für den angegebenen ARN	Schreiben	Encoder-Configuration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeletePlaybackKeyPair	Gewährt die Berechtigung zum Löschen des Wiedergabe-Schlüsselpaars für einen angegebenen ARN	Schreiben	Playback-Key-Pair*		
DeletePlaybackRestrictionPolicy	Gewährt die Berechtigung zum Löschen der Wiedergabe-Einschränkungsrichtlinie für einen angegebenen ARN	Schreiben	Playback-Restriction-Policy*		
DeleteRecordingConfiguration	Gewährt die Berechtigung zum Löschen einer Aufzeichnungskonfiguration für den angegebenen ARN	Schreiben	Recording-Configuration*		
DeleteStage	Gewährt die Berechtigung zum Löschen der Stufe für einen angegebenen ARN	Schreiben	Stage*		
DeleteStorageConfiguration	Gewährt die Berechtigung zum Löschen einer Speicherkonfiguration für den angegebenen ARN	Schreiben	Storage-Configuration*		
DeleteStreamKey	Gewährt die Berechtigung zum Löschen des Stream-Schlüssels für einen angegebenen ARN	Schreiben	Stream-Key*		
DisconnectParticipant	Gewährt die Berechtigung zum Trennen eines Teilnehmers für den angegebenen Stufen-ARN	Schreiben	Stage*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetChannel	Gewährt die Berechtigung zum Abrufen der Kanalkonfiguration für einen angegebenen Kanal-ARN	Lesen	Channel*		
GetComposition	Gewährt die Berechtigung zum Abrufen der Komposition für den angegebenen ARN	Lesen	Composition*		
GetEncoderConfiguration	Gewährt die Berechtigung zum Abrufen der Encoder-Konfiguration für den angegebenen ARN	Lesen	Encoder-Configuration*		
GetParticipant	Gewährt die Berechtigung, Teilnehmerinformationen für einen Stufen-ARN, eine Stufensitzung und einen Stufenteilnehmer abzurufen	Lesen	Stage*		
GetPlaybackKeyPair	Gewährt die Berechtigung, die Wiedergabe-Schlüsselpaar-Informationen für einen angegebenen ARN abzurufen	Lesen	Playback-Key-Pair*		
GetPlaybackRestrictionPolicy	Gewährt die Berechtigung zum Abrufen der Wiedergabeeinschränkungsrichtlinie für einen angegebenen ARN	Lesen	Playback-Restriction-Policy*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetRecordingConfiguration	Gewährt die Berechtigung zum Abrufen der Aufzeichnungskonfiguration für den angegebenen ARN	Lesen	Recording-Configuration*		
GetStage	Gewährt die Berechtigung zum Abrufen von Stufeninformationen für einen angegebenen ARN	Lesen	Stage*		
GetStageSession	Gewährt die Berechtigung, Stufensitzungsinformationen für einen Stufen-ARN und eine Stufensitzung abzurufen	Lesen	Stage*		
GetStorageConfiguration	Gewährt die Berechtigung zum Abrufen der Speicherkonfiguration für den angegebenen ARN	Lesen	Storage-Configuration*		
GetStream	Gewährt die Berechtigung zum Abrufen von Informationen über den aktiven (Live-) Stream auf einem bestimmten Kanal	Read	Channel*		
GetStreamKey	Gewährt die Berechtigung zum Abrufen von Stream-Schlüsselinformationen für einen angegebenen ARN	Lesen	Stream-Key*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetStreamSession	Gewährt die Berechtigung zum Abrufen von Informationen über die Stream-Sitzung auf einem angegebenen Kanal	Lesen	Channel*		
ImportPlaybackKeyPair	Gewährt die Berechtigung zum Importieren des öffentlichen Schlüssels.	Write	Playback-Key-Pair*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ListChannels	Gewährt die Berechtigung zum Abrufen von zusammenfassenden Informationen zu Kanälen	Auflisten	Channel*		
ListCompositions	Gewährt die Berechtigung zum Abrufen von zusammenden Informationen zu Kompositionen	Auflisten	Encoder-Configuration		
			Stage		
ListEncoderConfigurations	Gewährt die Berechtigung zum Abrufen von zusammenfassenden Informationen zu Encoder-Konfigurationen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListParticipantEvents	Gewährt die Berechtigung, Teilnehmerereignisse für einen Stufen-ARN, eine Stufensitzung und einen Stufenteilnehmer aufzulisten	Auflisten	Stage*		
ListParticipants	Gewährt die Berechtigung, Teilnehmer für einen Stufen-ARN und eine Stufensitzung aufzulisten	Auflisten	Stage*		
ListPlaybackKeyPairs	Gewährt die Berechtigung zum Abrufen von Zusammenfassungsinformationen zu Wiedergabe-Schlüsselpaaren	Auflisten	Playback-Key-Pair*		
ListPlaybackRestrictionPolicies	Gewährt die Berechtigung zum Abrufen von zusammenfassenden Informationen zu Wiedergabe-Einschränkungsrichtlinien	Auflisten			
ListRecordingConfigurations	Gewährt die Berechtigung zum Abrufen von zusammenfassenden Informationen zu Aufzeichnungskonfigurationen	Auflisten	Recording-Configuration*		
ListStageSessions	Gewährt die Berechtigung, Stufensitzungen für einen Stufen-ARN aufzulisten	Auflisten	Stage*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListStages	Gewährt die Berechtigung zum Abrufen von zusammenfassenden Informationen zu Stufen	Auflisten	Stage*		
ListStorageConfigurations	Gewährt die Berechtigung zum Abrufen von zusammenfassenden Informationen zu Speicherkonfigurationen	Auflisten			
ListStreamKeys	Gewährt die Berechtigung zum Abrufen von zusammenfassenden Informationen zu Stream-Schlüsseln	Auflisten	Channel* Stream-Key*		
ListStreamSessions	Gewährt die Berechtigung zum Abrufen von zusammenfassenden Informationen über die Stream-Sitzung auf einem angegebenen Kanal	Auflisten	Channel*		
ListStreams	Gewährt die Berechtigung, zusammenfassende Informationen zu Livestreams zu erhalten	List	Channel*		
ListTagsForResource	Gewährt die Berechtigung zum Abrufen von Informationen über die Tags für einen angegebenen ARN	Read	Channel Composition		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			Encoder-Configuration		
			Playback-Key-Pair		
			Playback-Restriction-Policy		
			Recording-Configuration		
			Stage		
			Storage-Configuration		
			Stream-Key		
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutMetadata	Gewährt die Berechtigung zum Einfügen von Metadaten in einen RTMP-Stream für einen angegebenen Kanal	Schreiben	Channel*		
StartComposition	Gewährt die Berechtigung zum Erstellen einer neuen Komposition	Schreiben	Encoder-Configuration*		
			Stage*		
			Channel		
			Storage-Configuration		
				aws:TagKeys aws:RequestTag/${TagKey}	
StartViewerSessionRevocation	Gewährt die Berechtigung, mit dem Widerruf der Viewer-Sitzung zu beginnen, die einem bestimmten Kanal-ARN und einer bestimmten Viewer-ID zugeordnet ist	Schreiben	Channel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopComposition	Gewährt die Berechtigung zum Anhalten der Komposition für den angegebenen ARN	Schreiben	Composition*		
StopStream	Gewährt die Berechtigung zum Trennen eines Streamers auf einem angegebenen Kanal	Write	Channel*		
TagResource	Gewährt die Berechtigung zum Hinzufügen oder Aktualisieren von Tags für eine Ressource mit einem angegebenen ARN	Markieren	Channel		
			Composition		
			Encoder-Configuration		
			Playback-Key-Pair		
			Playback-Restriction-Policy		
			Recording-Configuration		
			Stage		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			Storage-Configuration		
			Stream-Key		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags für eine Ressource mit einem angegebenen ARN	Markieren	Channel		
			Composition		
			Encoder-Configuration		
			Playback-Key-Pair		
			Playback-Restriction-Policy		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			Recording-Configuration		
			Stage		
			Storage-Configuration		
			Stream-Key		
				aws:TagKeys	
UpdateChannel	Gewährt die Berechtigung zum Aktualisieren der Konfiguration eines Kanals	Schreiben	Channel*		
UpdatePlaybackRestrictionPolicy	Gewährt die Berechtigung zum Aktualisieren einer Wiedergabeeinschränkungsrichtlinie für einen angegebenen ARN	Schreiben	Playback-Restriction-Policy*		
UpdateStage	Gewährt die Berechtigung zum Aktualisieren einer Stufenkonfiguration	Schreiben	Stage*		

Von Amazon Interactive Video Service definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Channel	`arn:${Partition}:ivs:${Region}:${Account}:channel/${ResourceId}`	aws:ResourceTag/${TagKey}
Stream-Key	`arn:${Partition}:ivs:${Region}:${Account}:stream-key/${ResourceId}`	aws:ResourceTag/${TagKey}
Playback-Key-Pair	`arn:${Partition}:ivs:${Region}:${Account}:playback-key/${ResourceId}`	aws:ResourceTag/${TagKey}
Playback-Restriction-Policy	`arn:${Partition}:ivs:${Region}:${Account}:playback-restriction-policy/${ResourceId}`	aws:ResourceTag/${TagKey}
Recording-Configuration	`arn:${Partition}:ivs:${Region}:${Account}:recording-configuration/${ResourceId}`	aws:ResourceTag/${TagKey}
Stage	`arn:${Partition}:ivs:${Region}:${Account}:stage/${ResourceId}`	aws:ResourceTag/${TagKey}
Composition	`arn:${Partition}:ivs:${Region}:${Account}:composition/${ResourceId}`	aws:ResourceTag/${TagKey}
Encoder-Configuration	`arn:${Partition}:ivs:${Region}:${Account}:encoder-configuration/${ResourceId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
Storage-Configuration	`arn:${Partition}:ivs:${Region}:${Account}:storage-configuration/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Interactive Video Service

Amazon Interactive Video Service definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Interactive Video Service Chat.

Amazon Interactive Video Service Chat (Servicepräfix: `ivschat`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Interactive Video Service Chat definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateChatToken	Gewährt die Berechtigung zum Erstellen eines verschlüsselten Tokens, das verwendet wird, um eine individuelle WebSocket Verbindung zu einem Raum herzustellen	Schreiben	Room*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateLoggingConfiguration	Gewährt die Berechtigung zum Erstellen einer Protokollierungskonfiguration, die es Clients ermöglicht, Nachrichten aufzuzeichnen	Schreiben	Logging-Configuration*		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey}	
CreateRoom	Gewährt die Berechtigung zum Erstellen eines Raums, der es Clients ermöglicht, Nachrichten zu verbinden und zu übergeben.	Schreiben	Room*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteLoggingConfiguration	Gewährt die Berechtigung zum Löschen einer Protokollierungskonfiguration für den angegebenen ARN der Protokollierungskonfiguration	Schreiben	Logging-Configuration*		
DeleteMessage	Gewährt die Berechtigung, ein Ereignis an einen bestimmten Raum zu senden, das Clients anweist, eine bestimmte Nachricht zu löschen.	Schreiben	Room*		
DeleteRoom	Gewährt die Berechtigung zum Löschen des Raums für einen angegebenen Raum-ARN.	Schreiben	Room*		
DisconnectUser	Gewährt die Berechtigung, alle Verbindungen mit einer angegebenen Benutzer-ID von einem Raum zu trennen.	Schreiben	Room*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetLoggingConfiguration	Gewährt die Berechtigung zum Abrufen der Protokollierungskonfiguration für einen angegebenen ARN der Protokollierungskonfiguration	Lesen	Logging-Configuration*		
GetRoom	Gewährt die Berechtigung zum Abrufen der Raumkonfiguration für einen angegebenen Raum-ARN.	Lesen	Room*		
ListLoggingConfigurations	Gewährt die Berechtigung zum Abrufen von zusammenfassenden Informationen zu Protokollierungskonfigurationen	Auflisten	Logging-Configuration*		
ListRooms	Gewährt die Berechtigung zum Abrufen von zusammenfassenden Informationen zu Räumen.	Auflisten	Room*		
ListTagsForResource	Gewährt die Berechtigung zum Abrufen von Informationen über die Tags für einen angegebenen ARN	Lesen	Room		
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SendEvent	Gewährt die Berechtigung, ein Ereignis an einen Raum zu senden.	Schreiben	Room*		
TagResource	Gewährt die Berechtigung zum Hinzufügen oder Aktualisieren von Tags für eine Ressource mit einem angegebenen ARN	Markieren	Logging-Configuration		
			Room		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags für eine Ressource mit einem angegebenen ARN	Tagging	Logging-Configuration		
			Room		
				aws:TagKeys	
UpdateLoggingConfiguration	Gewährt die Berechtigung zum Aktualisieren der Protokollierungskonfiguration für eine angegebene ARN der Protokollierungskonfiguration	Schreiben	Logging-Configuration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateRoom	Gewährt die Berechtigung zum Aktualisieren der Raumkonfiguration für einen angegebenen Raum-ARN.	Schreiben	Room*		

Von Amazon Interactive Video Service Chat definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Room	`arn:${Partition}:ivschat:${Region}:${Account}:room/${ResourceId}`	aws:ResourceTag/${TagKey}
Logging-Configuration	`arn:${Partition}:ivschat:${Region}:${Account}:logging-configuration/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Interactive Video Service Chat

Amazon Interactive Video Service Chat definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Invoicing Service

AWS Invoicing Service (Servicepräfix: `invoicing`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Invoicing Service definierte Aktionen
- Von AWS Invoicing Service definierte Ressourcentypen
- Bedingungsschlüssel für AWS Invoicing Service

Von AWS Invoicing Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetInvoiceEmailDeliveryPreferences [nur Berechtigung]	Gewährt die Berechtigung zum Erhalten der Einstellungen zur E-Mail-Zustellung von Rechnungen	Lesen			
GetInvoicePDF [nur Berechtigung]	Gewährt die Berechtigung zum Erhalten einer Rechnungs-PDF	Lesen			
ListInvoiceSummaries [nur Berechtigung]	Gewährt die Berechtigung zum Erhalten von zusammenfassenden Rechnungsinformationen für Ihr Konto oder Ihr verknüpftes Konto	Lesen			
PutInvoiceEmailDeliveryPreferences [nur Berechtigung]	Gewährt die Berechtigung zum Eingeben der Einstellungen zur E-Mail-Zustellung von Rechnungen	Schreiben			

Von AWS Invoicing Service definierte Ressourcentypen

AWS Invoicing Service unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf AWS Invoicing Service zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Invoicing Service

Invoicing Service hat keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT

AWS IoT (Servicepräfix: `iot`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS IoT definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung

mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptCertificateTransfer	Gewährt die Erlaubnis zum Akzeptieren einer ausstehenden Zertifikatübertragung.	Schreiben	cert*		
AddThingToBillingGroup	Gewährt die Berechtigung zum Hinzufügen der angegebenen Fakturierungsgruppe zu einem Objekt.	Schreiben	billinggroup*		
			thing*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddThingToThingGroup	Gewährt die Berechtigung zum Hinzufügen des Objekts zur angegebenen Objektgruppe.	Schreiben	thing*		
			thinggroup*		
AssociateTargetsWithJob	Gewährt die Erlaubnis zum Verknüpfen einer Gruppe mit einem kontinuierlichen Auftrag.	Schreiben	job*		
			thing*		
			thinggroup*		
AttachPolicy	Gewährt die Berechtigung zum Anfügen einer Richtlinie an das angegebene Ziel.	Berechtigungsverwaltung	cert		
			thinggroup		
AttachPrincipalPolicy	Gewährt die Berechtigung zum Anhängen der angegebenen Richtlinie an den angegebenen Prinzipal (Zertifikat oder andere Anmeldeinformationen).	Berechtigungsverwaltung	cert		
AttachSecurityProfile	Gewährt die Berechtigung zum Zuordnen eines Device-Defender-Sicherheitsprofils zu einer Objektgruppe oder diesem Konto.	Schreiben	securityprofile*		
			custommetric		
			dimension		
			thinggroup		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AttachThingPrincipal	Gewährt die Berechtigung zum Anhängen des angegebenen Prinzipals an das angegebene Objekt.	Schreiben			
CancelAuditMitigationActionsTask	Gewährt die Berechtigung zum Abbrechen einer laufenden Abhilfemaßnahme.	Schreiben			
CancelAuditTask	Gewährt die Erlaubnis zum Abbrechen eines laufenden Audits. Es kann sich um einen planmäßigen oder um einen On-Demand-Audit handeln.	Schreiben			
CancelCertificateTransfer	Gewährt die Berechtigung zum Abbrechen einer ausstehenden Weiterleitung für das angegebene Zertifikat.	Schreiben	cert*		
CancelDetectMitigationActionsTask	Gewährt die Berechtigung zum Abbrechen einer Gegenmaßnahme gegen Device Defender ML Detect.	Schreiben			
CancelJob	Gewährt die Berechtigung zum Abbrechen einer Aufgabe.	Schreiben	job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelJobExecution	Gewährt die Berechtigung zum Abbrechen einer Auftragsausführung auf einem bestimmten Gerät.	Schreiben	job*		
			thing*		
ClearDefaultAuthorizer	Gewährt die Berechtigung zum Löschen des Standardgenehmigers.	Schreiben			
CloseTunnel	Gewährt die Erlaubnis zum Schließen eines Tunnels.	Schreiben	tunnel*		
				iot:Delete	
ConfirmTopicRuleDestination	Gewährt die Berechtigung zum Bestätigen einer HTTP-URL TopicRuleDestinationDestination	Schreiben	destination*		
Connect	Gewährt die Berechtigung zur Verbindung als der angegebene Client	Schreiben	client*		
CreateAuditSuppression	Gewährt die Berechtigung zum Erstellen einer Device-Defender-Auditunterdrückung.	Schreiben			
CreateAuthorizer	Gewährt die Berechtigung zum Erstellen eines Genehmigers.	Schreiben	authorizer*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBillingGroup	Gewährt die Berechtigung zum Erstellen einer Fakturierungsgruppe.	Schreiben	billinggroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCertificateFromCsr	Gewährt die Berechtigung zum Erstellen eins X.509-Zertifikats mit der angegebenen Zertifikatsignaturanforderung.	Schreiben			
CreateCertificateProvider	Gewährt die Berechtigung zum Erstellen eines Zertifikatanbieters	Schreiben	certificateprovider*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCustomMetric	Gewährt die Berechtigung zum Erstellen einer benutzerdefinierten Metrik für gerätespezifische Metrikberichte und -überwachung.	Schreiben	custommetric*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDimension	Gewährt die Berechtigung zum Definieren einer Dimension, mit der der Umfang einer Metrik, die in einem Sicherheitsprofil verwendet wird, eingeschränkt werden kann.	Schreiben	dimension*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDomainConfiguration	Gewährt die Berechtigung zum Erstellen einer Domain-Konfiguration	Schreiben	domainconfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys iot:DomainName	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDynamicThingGroup	Gewährt die Berechtigung zum Erstellen einer Dynamic Thing Group	Write	dynamicthinggroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFleetMetric	Gewährt die Berechtigung zum Erstellen einer Flottenmetrik	Schreiben	fleetmetric*		
			index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateJob	Gewährt die Berechtigung zum Erstellen eines Auftrags.	Schreiben	job*		
			thing*		
			thinggroup*		
			jobtemplate		
			package		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			packageversion		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateJobTemplate	Gewährt die Berechtigung zum Erstellen einer Auftragsvorlage.	Schreiben	jobtemplate*		
			job		
			package		
			packageversion		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateKeysAndCertificate	Gewährt die Berechtigung zum Erstellen eines 2048-Bit-RSA-Schlüsselpaars und gibt ein X.509-Zertifikat unter Verwendung des ausgegebenen öffentlichen Schlüssels aus.	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateMitigationAction	Gewährt die Berechtigung zum Definieren einer Aktion, die mithilfe von auf Prüfungsergebnisse angewendet werden kann StartAuditMitigationActionsTask	Schreiben	mitigationaction*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateOTAUpdate	Gewährt die Berechtigung zum Erstellen eines OTA-Aktualisierungsauftrags.	Schreiben	otaupdate*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePackage	Gewährt die Berechtigung zum Erstellen eines Softwarepakets zum Bereitstellen auf Ihren Geräten	Schreiben	package*		iot:GetIndexingConfiguration
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreatePackageVersion	Gewährt die Berechtigung zum Erstellen einer Version unter dem angegebenen Paket	Schreiben	package*		iot:GetIndexingConfiguration
			packageversion*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePolicy	Gewährt die Berechtigung zum Erstellen einer AWS-IoT-Richtlinie	Schreiben	policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePolicyVersion	Gewährt die Berechtigung zum Erstellen einer neuen Version der angegebenen AWS-IoT-Richtlinie	Schreiben	policy*		
CreateProvisioningClaim	Gewährt die Berechtigung zum Erstellen eines Bereitstellungsantrags.	Schreiben	provisioningtemplate*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateProvisioningTemplate	Gewährt die Berechtigung zum Erstellen einer Vorlage für die Flottenbereitstellung.	Schreiben	provisioningtemplate*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProvisioningTemplateVersion	Gewährt die Berechtigung zum Erstellen einer neuen Version einer Flottenbereitstellungsvorlage.	Schreiben	provisioningtemplate*		
CreateRoleAlias	Gewährt die Berechtigung zum Erstellen eines Rollenalias.	Schreiben	rolealias*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScheduledAudit	Gewährt die Berechtigung zum Erstellen eines geplanten Audit, der in einem bestimmten Zeitintervall ausgeführt wird.	Schreiben	scheduledaudit*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSecurityProfile	Gewährt die Berechtigung zum Erstellen eines Device-Defender-Sicherheitsprofils.	Schreiben	securityprofile*		
			custommetric		
			dimension		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStream	Gewährt die Berechtigung zum Erstellen eines neuen AWS-IoT-Streams	Schreiben	stream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateThing	Gewährt die Erlaubnis zum Erstellen eines Objekts im Objektverzeichnis.	Schreiben	thing*		
			billinggroup		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateThingGroup	Gewährt die Berechtigung zum Erstellen einer neuen Objektgruppe.	Schreiben	thinggroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateThingType	Gewährt die Berechtigung zum Erstellen eines neuen Objekttyps.	Schreiben	thingtype*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTopicRule	Gewährt die Berechtigung zum Erstellen einer Regel.	Schreiben	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTopicRuleDestination	Gewährt die Berechtigung zum Erstellen eines TopicRule Destination	Schreiben	destination*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteAccountAuditConfiguration	Gewährt die Berechtigung zum Löschen der mit dem Konto verknüpften Auditkonfiguration.	Schreiben			
DeleteAuditSuppression	Gewährt die Berechtigung zum Löschen einer Device-Defender-Auditunterdrückung.	Schreiben			
DeleteAuthorizer	Gewährt die Berechtigung zum Löschen des angegebenen Genehmigers.	Schreiben	authorizer*		
DeleteBillingGroup	Gewährt die Berechtigung zum Löschen der angegebenen Fakturierungsgruppe.	Schreiben	billinggroup*		
DeleteCACertificate	Gewährt die Berechtigung zum Löschen eines registrierten CA-Zertifikats.	Schreiben	cacert*		
DeleteCertificate	Gewährt die Berechtigung zum Löschen des angegebenen Zertifikats	Schreiben	cert*		
DeleteCertificateProvider	Gewährt die Berechtigung zum Löschen eines Zertifikatanbieters	Schreiben	certificateprovider*		
DeleteCustomMetric	Gewährt die Berechtigung zum Löschen der angegebenen benutzerdefinierten Metrik aus Ihrem AWS-Konto	Schreiben	custommetric*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteDimension	Gewährt die Berechtigung zum Entfernen der angegebenen Dimension aus Ihrem AWS-Konto	Schreiben	dimension*		
DeleteDomainConfiguration	Gewährt die Berechtigung zum Löschen einer Domain-Konfiguration	Schreiben	domainconfiguration*		
DeleteDynamicThingGroup	Gewährt die Berechtigung zum Löschen der angegebenen Dynamic Thing Group	Write	dynamicthinggroup*		
DeleteFleetMetric	Gewährt die Berechtigung zum Löschen der angegebenen Flottenmetrik.	Schreiben	fleetmetric*		
DeleteJob	Gewährt die Berechtigung zum Löschen eines Auftrags und der damit verbundenen Auftragsausführungen.	Schreiben	job*		
DeleteJobExecution	Gewährt die Berechtigung zum Löschen einer Auftragsausführung.	Schreiben	job* thing*		
DeleteJobTemplate	Gewährt die Berechtigung zum Löschen einer Auftragsvorlage.	Schreiben	jobtemplate*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteMitigationAction	Gewährt die Berechtigung zum Löschen einer definierten Abhilfemaßnahme aus Ihrem AWS-Konto	Schreiben	mitigationaction*		
DeleteOTAUpdate	Gewährt die Berechtigung zum Löschen eines OTA-Aktualisierungsauftrags.	Schreiben	otaupdate*		
DeletePackage	Gewährt die Berechtigung zum Löschen eines Pakets	Schreiben	package*		
DeletePackageVersion	Gewährt die Berechtigung zum Löschen einer Version des angegebenen Pakets	Schreiben	package*		
			packageversion*		
DeletePolicy	Gewährt die Berechtigung, die angegebene Richtlinie zu löschen.	Schreiben	policy*		
DeletePolicyVersion	Gewährt die Berechtigung zum Löschen der angegebenen Version der angegebenen Richtlinie.	Schreiben	policy*		
DeleteProvisioningTemplate	Gewährt die Berechtigung zum Löschen einer Vorlage für die Flottenbereitstellung.	Schreiben	provisioningtemplate*		
DeleteProvisioningTemplateVersion	Gewährt die Berechtigung zum Löschen einer Version der Flottenbereitstellungsvorlage.	Schreiben	provisioningtemplate*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteRegistrationCode	Gewährt die Berechtigung zum Löschen eines Registrierungscodes für CA-Zertifikate.	Schreiben			
DeleteRoleAlias	Gewährt die Berechtigung zum Löschen der angegebenen Rollenalias.	Schreiben	rolealias*		
DeleteScheduledAudit	Gewährt die Berechtigung zum Löschen eines geplanten Audits.	Schreiben	scheduledaudit*		
DeleteSecurityProfile	Gewährt die Berechtigung zum Löschen eines Device-Defender-Sicherheitsprofils.	Schreiben	securityprofile*		
			custommetric		
			dimension		
DeleteStream	Gewährt die Berechtigung zum Löschen eines angegebenen Streams.	Schreiben	stream*		
DeleteThing	Gewährt die Berechtigung zum Löschen des angegebenen Objekts.	Schreiben	thing*		
DeleteThingGroup	Gewährt die Berechtigung zum Löschen der angegebenen Objektgruppe.	Schreiben	thinggroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteThingShadow	Gewährt die Berechtigung zum Löschen des angegebenen Objektschattens.	Schreiben	thing*		
DeleteThingType	Gewährt die Berechtigung zum Löschen des angegebenen Objekttyps.	Schreiben	thingtype*		
DeleteTopicRule	Gewährt die Berechtigung zum Löschen der angegebenen Regel.	Schreiben	rule*		
DeleteTopicRuleDestination	Gewährt die Berechtigung zum Löschen eines TopicRule Destination	Schreiben	destination*		
DeleteV2LoggingLevel	Gewährt die Berechtigung zum Löschen der angegebenen v2-Protokollierungsstufe.	Schreiben			
DeprecateThingType	Gewährt die Berechtigung zum Verwerten des angegebenen Objekttyps.	Schreiben	thingtype*		
DescribeAccountAuditConfiguration	Gewährt die Berechtigung zum Abrufen von Informationen über Audit-Konfigurationen für das Konto.	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeAuditFinding	Gewährt die Berechtigung zum Abrufen von Informationen zu einem einzelnen Audit-Ergebnis. Zu den Eigenschaften gehören der Grund für die Nichteinhaltung, der Schweregrad des Problems und der Zeitpunkt, zu dem der Audit gestartet wurde, der das Ergebnis zurückgab.	Lesen			
DescribeAuditMitigationActionsTask	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Audit-Abhilfeaufgabe, die verwendet wird, um Abhilfemaßnahmen auf eine Reihe von Audit-Ergebnissen anzuwenden.	Lesen			
DescribeAuditSuppression	Gewährt die Berechtigung zum Abrufen von Informationen über eine Auditunterdrückung von Device Defender	Lesen			
DescribeAuditTask	Gewährt die Berechtigung zum Abrufen von Informationen über ein Device-Defender-Audit.	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeAuthorizer	Gewährt die Berechtigung zum Beschreiben eines Genehmigers.	Lesen	authorizer*		
DescribeBillingGroup	Gewährt die Berechtigung zum Abrufen von Informationen über die angegebene Fakturierungsgruppe.	Lesen	billinggroup*		
DescribeCACertificate	Gewährt die Erlaubnis zum Beschreiben eines registrierten CA-Zertifikats.	Lesen	cacert*		
DescribeCertificate	Gewährt die Berechtigung zum Abrufen von Informationen über das angegebene Zertifikat.	Lesen	cert*		
DescribeCertificateProvider	Gewährt die Berechtigung zum Beschreiben eines Zertifikatanbieters	Lesen	certificateprovider*		
DescribeCustomMetric	Gewährt die Berechtigung zum Beschreiben einer benutzerdefinierten Metrik, die in Ihrem AWS-Konto definiert ist	Lesen	custommetric*		
DescribeDefaultAuthorizer	Gewährt die Berechtigung zum Beschreiben des Standardgenehmigers.	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDetectMitigationActionsTask	Gewährt die Erlaubnis, eine Gegenmaßnahme gegen Device Defender ML Detect zu beschreiben.	Lesen			
DescribeDimension	Gewährt die Berechtigung zum Abrufen von Details zu einer Dimension, die in Ihrem AWS-Konto definiert ist	Lesen	dimension*		
DescribeDomainConfiguration	Gewährt die Berechtigung zum Abrufen von Informationen über die Domain-Konfiguration	Lesen	domainconfiguration*		
DescribeEndpoint	Gewährt die Berechtigung zum Abrufen eines eindeutigen Endpunkts, der zum AWS-Konto gehört, das den Aufruf vornimmt	Lesen			
DescribeEventConfigurations	Gewährt die Berechtigung zum Abrufen von Kontoereigniskonfigurationen.	Lesen			
DescribeFleetMetric	Gewährt die Berechtigung zum Abrufen von Informationen über die angegebene Flottenmetrik.	Lesen	fleetmetric*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeIndex	Gewährt die Berechtigung zum Abrufen von Informationen über den angegebenen Index.	Lesen	index*		
DescribeJob	Gewährt die Berechtigung zum Beschreiben einer Aufgabe	Lesen	job*		
DescribeJobExecution	Gewährt die Berechtigung zum Beschreiben der Aufgabenausführung.	Lesen	job		
			thing		
DescribeJobTemplate	Gewährt die Berechtigung zum Beschreiben einer Auftragsvorlage.	Lesen	jobtemplate*		
DescribeManagedJobTemplate	Gewährt die Berechtigung zum Beschreiben einer verwalteten Auftragsvorlage	Lesen	jobtemplate*		
DescribeMitigationAction	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Abhilfemaßnahme.	Lesen	mitigationaction*		
DescribeProvisioningTemplate	Gewährt die Berechtigung zum Abrufen von Informationen über eine Vorlage für die Bereitstellung von Flotten.	Lesen	provisioningtemplate*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeProvisioningTemplateVersion	Gewährt die Berechtigung zum Abrufen von Informationen über eine Version der Flottenbereitstellung.	Lesen	provisioningtemplate*		
DescribeRoleAlias	Gewährt die Berechtigung zum Beschreiben eines Rollenalias.	Lesen	rolealias*		
DescribeScheduledAudit	Gewährt die Berechtigung zum Abrufen von Informationen zu einem geplanten Audit.	Lesen	scheduledaudit*		
DescribeSecurityProfile	Gewährt die Berechtigung zum Abrufen von Informationen über ein Device-Defender-Sicherheitsprofil.	Lesen	securityprofile*		
DescribeStream	Gewährt die Berechtigung zum Abrufen von Informationen über den angegebenen Stream.	Lesen	stream*		
DescribeThing	Gewährt die Berechtigung zum Abrufen von Informationen über das angegebene Objekt.	Lesen	thing*		
DescribeThingGroup	Gewährt die Berechtigung zum Abrufen von Informationen über die angegebenen Objektgruppe.	Lesen	thinggroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeThingRegistrationTask	Gewährt die Erlaubnis zum Abrufen von Informationen über die Massen-Objektregistrierungsaufgabe.	Lesen			
DescribeThingType	Gewährt die Berechtigung zum Abrufen von Informationen über den angegebenen Objekttyp.	Lesen	thingtype*		
DescribeTunnel	Gewährt die Berechtigung zum Beschreiben eines Tunnels.	Lesen	tunnel*		
DetachPolicy	Gewährt die Berechtigung zum Trennen einer Richtlinie von dem angegebenen Ziel.	Berechtigungsverwaltung	cert		
			thinggroup		
DetachPrincipalPolicy	Gewährt die Berechtigung zum Entfernen der angegebenen Richtlinie aus dem angegebenen Zertifikat.	Berechtigungsverwaltung	cert		
DetachSecurityProfile	Gewährt die Berechtigung zum Trennen der Mapping eines Device-Defender-Sicherheitsprofils von einer Objektgruppe oder diesem Konto.	Schreiben	securityprofile*		
			custommetric		
			dimension		
			thinggroup		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DetachThingPrincipal	Gewährt die Berechtigung zum Trennen des angegebenen Prinzipals von dem angegebenen Objekt.	Schreiben			
DisableTopicRule	Gewährt die Berechtigung zum Deaktivieren der angegebenen Regel.	Schreiben	rule*		
EnableTopicRule	Gewährt die Berechtigung zum Aktivieren der angegebenen Regel.	Schreiben	rule*		
GetBehaviorModelTrainingSummaries	Gewährt die Berechtigung, den Status des ML-Detect-Sicherheitsprofil-Trainingsmodells eines Device Defender abzurufen.	Auflisten	securityprofile		
GetBucketsAggregation	Gewährt die Erlaubnis zum Erhalten von Bucket-Aggregation für den IoT-Flottenindex	Read	index*		
GetCardinality	Gewährt die Erlaubnis zum Erhalten von Kardinalität für den IoT-Flottenindex	Lesen	index*		
GetEffectivePolicies	Gewährt die Erlaubnis zum Erhalten von effektiven Richtlinien.	Lesen	cert		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetIndexingConfiguration	Gewährt die Berechtigung zum Abrufen der aktuellen Flottenindexierungskonfiguration	Lesen			
GetJobDocument	Gewährt die Erlaubnis zum Abrufen eines Auftragsdokuments.	Lesen	job*		
GetLoggingOptions	Gewährt die Berechtigung zum Abrufen der Protokollierungsoptionen.	Lesen			
GetOTAUpdate	Gewährt die Berechtigung zum Abrufen von Informationen über den OTA-Aktualisierungsauftrag.	Lesen	otaupdate*		
GetPackage	Gewährt die Berechtigung zum Abrufen der Informationen zu den Paketen	Lesen	package*		
GetPackageConfiguration	Gewährt die Berechtigung zum Abrufen der Paketkonfiguration des Kontos	Lesen			
GetPackageVersion	Gewährt die Berechtigung zum Abrufen der Version des Pakets	Lesen	package*		
			packageversion*		
GetPercentiles	Gewährt die Erlaubnis zum Abrufen von Perzentilen für den IoT-Flottenindex	Lesen	index*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetPolicy	Gewährt die Berechtigung zum zum Abrufen von Informationen zu der angegebenen Richtlinie mit dem Richtliniendokument der Standard-Version.	Lesen	policy*		
GetPolicyVersion	Gewährt die Berechtigung zum Abrufen von Informationen über die angegebene Richtlinienversion.	Lesen	policy*		
GetRegistrationCode	Gewährt die Berechtigung zum Abrufen eines Registrierungscodes für die Registrierung eines CA-Zertifikats bei AWS IoT	Lesen			
GetRetainedMessage	Gewährt die Berechtigung zum Abrufen der gespeicherten Nachricht zum angegebenen Thema	Lesen	topic*		
GetStatistics	Gewährt Erlaubnis zum Abrufen von Statistiken für den IoT-Flottenindex	Lesen	index*		
GetThingShadow	Gewährt die Berechtigung zum Abrufen des Objektschattens.	Lesen	thing*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetTopicRule	Gewährt die Berechtigung zum Abrufen von Informationen über die angegebene Regel.	Lesen	rule*		
GetTopicRuleDestination	Gewährt die Berechtigung zum Abrufen eines TopicRule Destination	Lesen	destination*		
GetV2LoggingOptions	Gewährt die Berechtigung zum Abrufen von v2-Protokollierungsoptionen.	Lesen			
ListActiveViolations	Gewährt die Berechtigung zum Auflisten der aktiven Verstöße für ein bestimmtes Device-Defender-Sicherheitsprofil oder -Objekt.	Auflisten	securityprofile		
			thing		
ListAttachedPolicies	Gewährt die Berechtigung zum Auflisten der Richtlinien, die der angegebenen Objektgruppe zugeordnet sind.	Auflisten			
ListAuditFindings	Gewährt die Berechtigung zum Auflisten der Ergebnisse eines Device-Defender-Audits oder der während eines bestimmten Zeitraums durchgeführten Audits.	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAuditMitigationActionsExecutions	Gewährt die Berechtigung zum Abrufen des Status von Audit-Abhilfemaßnahmen, die ausgeführt wurden.	Auflisten			
ListAuditMitigationActionsTasks	Gewährt die Berechtigung zum Abrufen einer Liste von Prüfungs/Abhilfemaßnahmen-Aufgaben, die den angegebenen Filterkriterien entsprechen.	Auflisten			
ListAuditSuppressions	Gewährt die Berechtigung zum Auflisten Ihrer Auditunterdrückungen von Device Defender.	Auflisten			
ListAuditTasks	Gewährt die Berechtigung zum Auflisten der Device-Defender-Audits, die während eines bestimmten Zeitraums durchgeführt wurden.	Auflisten			
ListAuthorizers	Gewährt die Erlaubnis zum Auflisten der Genehmiger, die in Ihrem Konto registriert sind.	Auflisten			
ListBillingGroups	Gewährt die Berechtigung zum Auflisten aller Fakturierungsgruppen.	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListCACertificates	Gewährt die Berechtigung zum Auflisten die für Ihr AWS-Konto registrierten CA-Zertifikate	Auflisten			
ListCertificateProviders	Gewährt die Berechtigung zum Auflisten von Zertifikatanbietern im Konto	Auflisten			
ListCertificates	Gewährt die Erlaubnis zum Auflisten Ihrer Zertifikate.	Auflisten			
ListCertificatesByCA	Gewährt die Berechtigung zum Auflisten der von dem angegebenen CA-Zertifikat signierten Gerätezertifikate.	Auflisten			
ListCustomMetrics	Gewährt die Berechtigung zum Auflisten der benutzerdefinierten Metriken in Ihrem AWS-Konto	Auflisten			
ListDetectMitigationActionsExecutions	Gewährt die Berechtigung zum Auflisten von Ausführungen von Gegenmaßnahmen für ein Device-Defender-ML-Sicherheitsprofil.	Auflisten	thing		
ListDetectMitigationActionsTasks	Gewährt die Erlaubnis zum Auflisten von Gegenmaßnahmenaufgaben gegen Device Defender ML Detect.	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDimensions	Gewährt die Berechtigung zum Auflisten der Dimensionen, die für Ihr AWS-Konto definiert sind	Auflisten			
ListDomainConfigurations	Gewährt die Berechtigung zum Auflisten der von Ihrem AWS-Konto erstellten Domain-Konfiguration	Auflisten			
ListFleetMetrics	Gewährt die Berechtigung zum Auflisten der Flottenmetriken in Ihrem Konto.	Auflisten			
ListIndices	Gewährt die Erlaubnis zum Auflisten aller Indizes für den Flottenindex	Auflisten			
ListJobExecutionsForJob	Gewährt die Berechtigung zum Auflisten von Auftragsausführungen für einen Auftrag.	Auflisten	job*		
ListJobExecutionsForThing	Gewährt die Berechtigung zum Auflisten der Auftragsausführungen für das angegebene Objekt.	Auflisten	thing*		
ListJobTemplates	Gewährt die Berechtigung zum Auflisten von Auftragsvorlagen.	Auflisten			
ListJobs	Gewährt die Berechtigung zum Auflisten von Aufträgen.	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListManagedJobTemplates	Gewährt die Berechtigung zum Auflisten von verwalteten Auftragsvorlagen	Auflisten			
ListMetricValues	Gewährt Berechtigungen zum Auflisten der Metrikwerte für ein Objekt auf der Grundlage des metricName und der Dimension, falls angegeben	Auflisten	thing*		
ListMitigationActions	Gewährt die Berechtigung zum Abrufen einer Liste aller Abhilfemaßnahmen, die den angegebenen Filterkriterien entsprechen.	Auflisten			
ListNamedShadowsForThing	Gewährt die Erlaubnis zum Auflisten aller benannten Schatten für ein bestimmtes Objekt.	Auflisten	thing*		
ListOTAUpdates	Gewährt die Berechtigung zum Auflisten von OTA-Aktualisierungsaufträgen im Konto.	Auflisten			
ListOutgoingCertificates	Gewährt die Erlaubnis zum Auflisten von Zertifikaten, die übertragen, aber noch nicht akzeptiert wurden.	Auflisten			
ListPackageVersions	Gewährt die Berechtigung zum Auflisten der Versionen für ein Paket im Konto	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListPackages	Gewährt die Berechtigung zum Auflisten der Pakete im Konto	Auflisten			
ListPolicies	Gewährt die Erlaubnis zum Auflisten Ihrer Richtlinien.	Auflisten			
ListPolicyPrincipals	Gewährt die Berechtigung zum Auflisten der Prinzipale, die mit der angegebenen Richtlinie verknüpft sind.	Auflisten			
ListPolicyVersions	Gewährt die Berechtigung zum Auflisten der Versionen der angegebenen Richtlinie und identifiziert die Standardversion.	Auflisten	policy*		
ListPrincipalPolicies	Gewährt die Berechtigung zum Auflisten der Richtlinien, die dem angegebenen Prinzipal zugeordnet sind. Wenn Sie eine Amazon Cognito-Identität verwenden, muss die ID das Amazon Cognito Identity-Format aufweisen.	Auflisten			
ListPrincipalThings	Gewährt die Berechtigung zum Auflisten der Objekte, die mit dem angegebenen Prinzipal verknüpft sind.	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListProvisioningTemplateVersions	Gewährt die Berechtigung zum Abrufen einer Liste von Versionen der Flottenbereitstellungsvorlagen.	Auflisten	provisioningtemplate*		
ListProvisioningTemplates	Gewährt die Berechtigung zum Auflisten der Vorlagen für die Flottenbereitstellung in Ihrem AWS-Konto	Auflisten			
ListRelatedResourcesForAuditFinding	Gewährt die Berechtigung zum Auflisten zugehöriger Ressourcen eines einzelnen Audit-Ergebnis	Auflisten			
ListRetainedMessages	Gewährt die Berechtigung zum Auflisten der aufbewahrten Nachrichten für Ihr Konto	Auflisten			
ListRoleAliases	Gewährt die Berechtigung zum Auflisten von Rollenaliasen.	Auflisten			
ListScheduledAudits	Gewährt die Erlaubnis zum Auflisten aller Ihrer geplanten Audits.	Auflisten			
ListSecurityProfiles	Gewährt die Berechtigung zum Auflisten der von Ihnen erstellten Device-Defender-Sicherheitsprofilen.	Auflisten	custommetric		
			dimension		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListSecurityProfilesForTarget	Gewährt die Berechtigung zum Auflisten der Device-Defender-Sicherheitsprofile, die einem Ziel zugeordnet sind.	Auflisten	thinggroup		
ListStreams	Gewährt die Berechtigung zum Auflisten der Streams in Ihrem Konto.	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen	authorizer		
			billinggroup		
			cacert		
			certificateprovider		
			custommetric		
			dimension		
			domainconfiguration		
			dynamicthinggroup		
			fleetmetric		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			job		
			jobtemplate		
			mitigationaction		
			otaupdate		
			policy		
			provisioningtemplate		
			rolealias		
			rule		
			scheduledaudit		
			securityprofile		
			stream		
			thinggroup		
			thingtype		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTargetsForPolicy	Gewährt die Berechtigung zum Auflisten von Zielen für die angegebene Richtlinie.	Auflisten	policy*		
ListTargetsForSecurityProfile	Gewährt die Berechtigung zum Auflisten der Ziele, die einem bestimmten Device-Defender-Sicherheitsprofil zugeordnet sind.	Auflisten	securityprofile*		
ListThingGroups	Gewährt die Berechtigung zum Auflisten aller Objektgruppen.	Auflisten			
ListThingGroupsForThing	Gewährt die Berechtigung zum Auflisten von Objektgruppen, zu denen das angegebene Objekt gehört.	Auflisten	thing*		
ListThingPrincipals	Gewährt die Berechtigung zum Auflisten der Prinzipale, die mit dem angegebenen Objekt verknüpft sind.	Auflisten			
ListThingRegistrationTaskReports	Gewährt die Erlaubnis zum Auflisten von Informationen über Massen-Objektregistrierungsaufgaben.	Auflisten			
ListThingRegistrationTasks	Gewährt die Erlaubnis zum Auflisten von Massen-Objektregistrierungsaufgaben.	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListThingTypes	Gewährt die Berechtigung zum Auflisten aller Objekttypen.	Auflisten			
ListThings	Gewährt die Berechtigung zum Auflisten aller Objekte.	Auflisten			
ListThingsInBillingGroup	Gewährt die Berechtigung zum Auflisten aller Objekte in der angegebenen Fakturierungsgruppe.	Auflisten	billinggroup*		
ListThingsInThingGroup	Gewährt die Berechtigung zum Auflisten aller Objekte in der angegebenen Objektgruppe.	Auflisten	thinggroup*		
ListTopicRuleDestinations	Gewährt die Berechtigung zum Auflisten aller TopicRule Destinations	Auflisten			
ListTopicRules	Gewährt die Erlaubnis zum Auflisten der Regeln für das angegebene Thema.	Auflisten			
ListTunnels	Gewährt die Berechtigung zum Auflisten von Tunneln.	Auflisten			
ListV2LoggingLevels	Gewährt die Berechtigung zum Auflisten der v2-Protokollierungsstufen.	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListViolationEvents	Gewährt die Berechtigung zum Auflisten der Verstöße gegen das Device-Defender-Sicherheitsprofil, die während des angegebenen Zeitraums erkannt wurden.	Auflisten	securityprofile		
			thing		
OpenTunnel	Gewährt die Erlaubnis zum Öffnen eines Tunnels.	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys iot:ThingGroupArn iot:TunnelDestinationService	
Publish	Gewährt die Berechtigung zum Veröffentlichen in dem angegebenen Thema.	Schreiben	topic*		
PutVerificationStateOnViolation	Gewährt die Berechtigung zur Vergabe eines Verifizierungsstatus für einen Verstoß	Schreiben			
Receive	Gewährt die Erlaubnis, von dem angegebenen Thema zu erhalten.	Schreiben	topic*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RegisterCACertificate	Gewährt die Berechtigung zum Registrieren eines CA-Zertifikats bei AWS IoT	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
RegisterCertificate	Gewährt die Berechtigung zum Registrieren eines Gerätezertifikats bei AWS IoT	Schreiben			
RegisterCertificateWithoutCA	Gewährt die Berechtigung zum Registrieren eines Gerätezertifikats bei AWS IoT ohne registrierte Zertifizierungsstelle	Schreiben			
RegisterThing	Gewährt die Berechtigung zum Registrieren Ihres Objekts.	Schreiben			
RejectCertificateTransfer	Gewährt die Erlaubnis zum Ablehnen einer ausstehenden Zertifikatübertragung.	Schreiben	cert*		
RemoveThingFromBillingGroup	Gewährt die Berechtigung zum Entfernen des Objekts aus der angegebenen Fakturierungsgruppe.	Schreiben	billinggroup* thing*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RemoveThingFromThingGroup	Gewährt die Berechtigung zum Entfernen des Objekts aus der angegebenen Objektgruppe.	Schreiben	thing*		
			thinggroup*		
ReplaceTopicRule	Gewährt die Berechtigung zum Ersetzen der angegebenen Regel.	Schreiben	rule*		
RetainPublish	Gewährt die Berechtigung zum Veröffentlichen einer gespeicherten Nachricht für das angegebene Thema	Schreiben	topic*		
RotateTunnelAccessToken	Erteilt die Berechtigung, das Zugriffstoken eines Tunnels zu drehen	Schreiben	tunnel*		
				iot:ThingGroupArn iot:TunnelDestinationService iot:ClientMode	
SearchIndex	Gewährt die Erlaubnis zum Durchsuchen des IoT-Flottenindex	Read	index*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SetDefaultAuthorizer	Gewährt die Berechtigung zum Festlegen des Standardgenehmigers. Dieser wird verwendet, wenn eine Websocket-Verbindung aufgebaut wird, ohne dass ein Genehmiger angegeben wird.	Berechtigungsverwaltung	authorizer*		
SetDefaultPolicyVersion	Gewährt die Berechtigung zum Festlegen der angegebenen Version der angegebenen Richtlinie als (operative) Standardversion der Richtlinie.	Berechtigungsverwaltung	policy*		
SetLoggingOptions	Gewährt die Berechtigung zum Festlegen der Protokollierungsoptionen.	Schreiben			
SetV2LoggingLevel	Gewährt die Berechtigung zum Festlegen der v2-Protokollierungsstufe.	Schreiben			
SetV2LoggingOptions	Gewährt die Berechtigung zum Festlegen der v2-Protokollierungsoptionen.	Schreiben			
StartAuditMitigationActionsTask	Gewährt die Berechtigung zum Starten einer Aufgabe, die eine Reihe von Abhilfemaßnahmen auf das angegebene Ziel anwendet.	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartDetectMitigationActionsTask	Gewährt die Berechtigung zum Starten einer Aufgabe zum Erkennen von Abhilfemaßnahmen von Device Defender ML.	Schreiben	securityprofile		
StartOnDemandAuditTask	Gewährt die Berechtigung zum Starten eines Device-Defender-Audits auf Anforderung.	Schreiben			
StartThingRegistrationTask	Gewährt die Erlaubnis zum Starten einer Massen-Objektregistrierungsaufgabe.	Schreiben			
StopThingRegistrationTask	Gewährt die Erlaubnis zum Beenden einer Massen-Objektregistrierungsaufgabe.	Schreiben			
Subscribe	Gewährt die Berechtigung zum Abonnieren des angegebenen TopicFilter	Schreiben	topicfilter*		
TagResource	Gewährt die Berechtigung zum Markieren einer angegebenen Ressourcen	Markieren	authorizer		
			billinggroup		
			cacert		
			certificateprovider		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			custommetric		
			dimension		
			domainconfiguration		
			dynamicthinggroup		
			fleetmetric		
			job		
			jobtemplate		
			mitigationaction		
			otaupdate		
			package		
			packageversion		
			policy		
			provisioningtemplate		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			rolealias		
			rule		
			scheduledaudit		
			securityprofile		
			stream		
			thinggroup		
			thingtype		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestAuthorization	Gewährt die Erlaubnis zum Testen der Auswertung der Richtlinien für Gruppenrichtlinien	Lesen	cert		
TestInvokeAuthorizer	Gewährt die Berechtigung zum Testaufrufen des angegebenen Lambda-Genehmigers zu Testzwecken.	Lesen	authorizer*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TransferCertificate	Gewährt die Berechtigung zum Übertragen des angegebenen Zertifikats auf das angegebene AWS-Konto	Schreiben	cert*		
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer angegebenen Ressource	Tagging	authorizer		
			billinggroup		
			cacert		
			certificateprovider		
			custommetric		
			dimension		
			domainconfiguration		
			dynamicthinggroup		
			fleetmetric		
			job		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			jobtemplate		
			mitigationaction		
			otaupdate		
			package		
			packageversion		
			policy		
			provisioningtemplate		
			rolealias		
			rule		
			scheduledaudit		
			securityprofile		
			stream		
			thinggroup		
			thingtype		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
UpdateAccountAuditConfiguration	Gewährt die Berechtigung zum Konfigurieren oder Neukonfigurieren der Audit-Einstellungen für Device Defender für dieses Konto.	Schreiben			
UpdateAuditSuppression	Gewährt die Berechtigung zum Aktualisieren einer Device-Defender-Auditunterdrückung.	Schreiben			
UpdateAuthorizer	Gewährt die Berechtigung zum Aktualisieren eines Genehmigers	Schreiben	authorizer*		
UpdateBillingGroup	Gewährt die Berechtigung zum Aktualisieren von Informationen, die der angegebenen Fakturierungsgruppe zugeordnet sind.	Schreiben	billinggroup*		
UpdateCACertificate	Gewährt die Berechtigung zum Aktualisieren eines registrierten CA-Zertifikats.	Schreiben	cacert*		iam:PassRole
UpdateCertificate	Gewährt die Berechtigung zum Aktualisieren des Status des angegebenen Zertifikats. Dieser Vorgang ist idempotent.	Schreiben	cert*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateCertificateProvider	Gewährt die Berechtigung zum Aktualisieren eines Zertifikatanbieters	Schreiben	certificateprovider*		
UpdateCustomMetric	Gewährt die Berechtigung zum Aktualisieren der angegebenen benutzerdefinierten Metrik.	Schreiben	custommetric*		
UpdateDimension	Gewährt die Berechtigung zum Aktualisieren der Definition für eine Dimension.	Schreiben	dimension*		
UpdateDomainConfiguration	Gewährt die Berechtigung zum Aktualisieren einer Domain-Konfiguration	Schreiben	domainconfiguration*		
UpdateDynamicThingGroup	Gewährt die Berechtigung zum Aktualisieren einer Dynamic Thing Group	Schreiben	dynamicthinggroup*		
UpdateEventConfigurations	Gewährt die Berechtigung zum Aktualisieren von Ereigniskonfigurationen.	Schreiben			
UpdateFleetMetric	Gewährt die Berechtigung zum Aktualisieren einer Flottenmetrik	Write	fleetmetric*		
			index*		
UpdateIndexingConfiguration	Gewährt die Berechtigung zum Aktualisieren der Flottenindexierungskonfiguration	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateJob	Gewährt die Berechtigung zum Aktualisieren eines Auftrags.	Schreiben	job*		
UpdateMitigationAction	Gewährt die Berechtigung zum Aktualisieren der Definition für die angegebene Abhilfemaßnahme.	Schreiben	mitigationaction*		
UpdatePackage	Gewährt die Berechtigung zum Aktualisieren eines Pakets	Schreiben	package*		iot:GetIndexingConfiguration
UpdatePackageConfiguration	Gewährt die Berechtigung zum Aktualisieren der Paketkonfiguration des Kontos	Schreiben			iam:PassRole
UpdatePackageVersion	Gewährt die Berechtigung zum Aktualisieren der Version des angegebenen Pakets	Schreiben	package*		iot:GetIndexingConfiguration
			packageversion*		
UpdateProvisioningTemplate	Gewährt die Berechtigung zum Aktualisieren einer Vorlage für die Flottenbereitstellung.	Schreiben	provisioningtemplate*		iam:PassRole
UpdateRoleAlias	Gewährt die Berechtigung zum Aktualisieren eines Rollenalias	Schreiben	rolealias*		iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateScheduledAudit	Gewährt die Berechtigung zum Aktualisieren eines geplanten Audits, einschließlich welche Prüfungen durchgeführt werden und wie oft der Audit stattfindet.	Schreiben	scheduledaudit*		
UpdateSecurityProfile	Gewährt die Berechtigung zum Aktualisieren eines Device-Defender-Sicherheitsprofils.	Schreiben	securityprofile*		
			custommetric		
			dimension		
UpdateStream	Gewährt die Berechtigung zum Aktualisieren der Daten für einen Stream.	Schreiben	stream*		
UpdateThing	Gewährt die Berechtigung zum Aktualisieren von Informationen im Zusammenhang mit dem angegebenen Objekt.	Schreiben	thing*		
UpdateThingGroup	Gewährt die Berechtigung zum Aktualisieren von Informationen, die mit der angegebenen Objektgruppe verknüpft sind.	Schreiben	thinggroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateThingGroupsForThing	Gewährt die Erlaubnis zum Aktualisieren der Objektgruppen, zu denen das Objekt gehört.	Schreiben	thing*		
			thinggroup		
UpdateThingShadow	Gewährt die Berechtigung zum Aktualisieren eines Objektschattens.	Schreiben	thing*		
UpdateTopicRuleDestination	Gewährt die Berechtigung zum Aktualisieren eines TopicRuleDestination	Schreiben	destination*		
ValidateSecurityProfileBehaviors	Gewährt die Berechtigung zum Überprüfen der Verhaltensspezifikation für das Device-Defender-Sicherheitsprofil.	Lesen			

Von AWS IoT definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
client	`arn:${Partition}:iot:${Region}:${Account}:client/${ClientId}`	

Ressourcentypen	ARN	Bedingungsschlüssel
index	arn:${Partition}:iot:${Region}:${Account}:index/${IndexName}	
fleetmetric	arn:${Partition}:iot:${Region}:${Account}:fleetmetric/${FleetMetricName}	aws:ResourceTag/${TagKey}
job	arn:${Partition}:iot:${Region}:${Account}:job/${JobId}	aws:ResourceTag/${TagKey}
jobtemplate	arn:${Partition}:iot:${Region}:${Account}:jobtemplate/${JobTemplateId}	aws:ResourceTag/${TagKey}
tunnel	arn:${Partition}:iot:${Region}:${Account}:tunnel/${TunnelId}	aws:ResourceTag/${TagKey}
thing	arn:${Partition}:iot:${Region}:${Account}:thing/${ThingName}	
thinggroup	arn:${Partition}:iot:${Region}:${Account}:thinggroup/${ThingGroupName}	aws:ResourceTag/${TagKey}
billinggroup	arn:${Partition}:iot:${Region}:${Account}:billinggroup/${BillingGroupName}	aws:ResourceTag/${TagKey}
dynamicthinggroup	arn:${Partition}:iot:${Region}:${Account}:thinggroup/${ThingGroupName}	aws:ResourceTag/${TagKey}
thingtype	arn:${Partition}:iot:${Region}:${Account}:thingtype/${ThingTypeName}	aws:ResourceTag/${TagKey}
topic	arn:${Partition}:iot:${Region}:${Account}:topic/${TopicName}	
topicfilter	arn:${Partition}:iot:${Region}:${Account}:topicfilter/${TopicFilter}	

Ressourcentypen	ARN	Bedingungsschlüssel
rolealias	arn:${Partition}:iot:${Region}:${Account}:rolealias/${RoleAlias}	aws:ResourceTag/${TagKey}
authorizer	arn:${Partition}:iot:${Region}:${Account}:authorizer/${AuthorizerName}	aws:ResourceTag/${TagKey}
policy	arn:${Partition}:iot:${Region}:${Account}:policy/${PolicyName}	aws:ResourceTag/${TagKey}
cert	arn:${Partition}:iot:${Region}:${Account}:cert/${Certificate}	
cacert	arn:${Partition}:iot:${Region}:${Account}:cacert/${CACertificate}	aws:ResourceTag/${TagKey}
stream	arn:${Partition}:iot:${Region}:${Account}:stream/${StreamId}	aws:ResourceTag/${TagKey}
otaupdate	arn:${Partition}:iot:${Region}:${Account}:otaupdate/${OtaUpdateId}	aws:ResourceTag/${TagKey}
scheduledaudit	arn:${Partition}:iot:${Region}:${Account}:scheduledaudit/${ScheduleName}	aws:ResourceTag/${TagKey}
mitigationaction	arn:${Partition}:iot:${Region}:${Account}:mitigationaction/${MitigationActionName}	aws:ResourceTag/${TagKey}
securityprofile	arn:${Partition}:iot:${Region}:${Account}:securityprofile/${SecurityProfileName}	aws:ResourceTag/${TagKey}
custommetric	arn:${Partition}:iot:${Region}:${Account}:custommetric/${MetricName}	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
dimension	arn:${Partition}:iot:${Region}:${Account}:dimension/${DimensionName}	aws:ResourceTag/${TagKey}
rule	arn:${Partition}:iot:${Region}:${Account}:rule/${RuleName}	aws:ResourceTag/${TagKey}
destination	arn:${Partition}:iot:${Region}:${Account}:destination/${DestinationType}/${Uuid}	
provisioningtemplate	arn:${Partition}:iot:${Region}:${Account}:provisioningtemplate/${ProvisioningTemplate}	aws:ResourceTag/${TagKey}
domainconfiguration	arn:${Partition}:iot:${Region}:${Account}:domainconfiguration/${DomainConfigurationName}/${Id}	aws:ResourceTag/${TagKey}
package	arn:${Partition}:iot:${Region}:${Account}:package/${PackageName}	aws:ResourceTag/${TagKey}
packageversion	arn:${Partition}:iot:${Region}:${Account}:package/${PackageName}/version/${VersionName}	aws:ResourceTag/${TagKey}
certificateprovider	arn:${Partition}:iot:${Region}:${Account}:certificateprovider/${CertificateProviderName}	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS IoT

AWS IoT definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch einen Tag-Schlüssel in der Anforderung.	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff durch eine Tag-Schlüsselkomponente eines Tags, das mit der IoT-Ressource in der Anforderung verknüpft ist.	String
aws:TagKeys	Filtert den Zugriff durch eine Liste von Tag-Schlüsseln, die mit der IoT-Ressource in der Anforderung verknüpft sind	ArrayOfString
iot:ClientMode	Filtert den Zugriff nach dem Modus des Clients für einen IoT-Tunnel	String
iot:Delete	Filtert den Zugriff nach einem Flag, das angibt, ob ein IoT-Tunnel auch sofort gelöscht werden soll, wenn iot:CloseTunnel request ausgeführt wird	Bool
iot:DomainName	Filtert den Zugriff basierend auf dem Domänennamen eines IoT DomainConfiguration	String
iot:ThingGroupArn	Filtert den Zugriff durch eine Liste von IoT-Thing-Gruppen-ARNs, zu denen das Ziel-IoT-Thing für einen IoT-Tunnel gehört	ArrayOfARN
iot:TunnelDestinationService	Filtert den Zugriff durch eine Liste von Zielservices für einen IoT-Tunnel	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT 1-Click

AWS IoT 1-Click (Servicepräfix: `iot1click`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS IoT 1-Click definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateDeviceWithPlacement	Gewährt die Berechtigung, ein Gerät einer Platzierung zuordnen	Write	project*		
ClaimDevicesByClaimCode	Gewährt die Berechtigung, einen Batch von Geräten mit einem Beantragungscode zu beantragen	Read			
CreatePlacement	Gewährt die Berechtigung zum Erstellen einer neuen Platzierung in einem Projekt	Write	project*		
CreateProject		Write	project*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Gewährt die Berechtigung zum Erstellen eines neuen Projekts			aws:RequestTag/${TagKey} aws:TagKeys	
DeletePlacement	Gewährt die Berechtigung zum Löschen einer Platzierung aus einem Projekt	Write	project*		
DeleteProject	Gewährt die Berechtigung zum Löschen eines Projekts	Write	project*		
DescribeDevice	Gewährt die Berechtigung, ein Gerät zu beschreiben	Read	device*		
DescribePlacement	Gewährt die Berechtigung zum Beschreiben einer Platzierung	Read	project*		
DescribeProject	Gewährt die Berechtigung zum Beschreiben eines Projekts	Read	project*		
DisassociateDeviceFromPlacement	Gewährt die Berechtigung, ein Gerät von einer Platzierung zu trennen	Write	project*		
FinalizeDeviceClaim	Gewährt die Berechtigung, eine Beantragung abzuschließen	Read	device*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
GetDeviceMethods	Gewährt die Berechtigung, verfügbare Methoden eines Geräts zu erhalten	Read	device*		
GetDevicesInPlacement	Gewährt die Berechtigung, Geräte zu erhalten, die einer Platzierung zugeordnet sind	Read	project*		
InitiateDeviceClaim	Gewährt die Berechtigung, eine Beantragung zu initialisieren	Read	device*		
InvokeDeviceMethod	Gewährt die Berechtigung zum Aufrufen einer Gerätemethode	Write	device*		
ListDeviceEvents	Gewährt die Berechtigung, vergangene Ereignisse aufzulisten, die von einem Gerät	Read	device*		
ListDevices	Gewährt die Berechtigung, alle Geräte aufzulisten	List			
ListPlacements	Gewährt die Berechtigung zum Auflisten von Platzierungen in einem Projekt	Read	project*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListProjects	Gewährt die Berechtigung zum Auflisten aller Projekte	List			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für eine Ressource	Read	device		
			project		
TagResource	Gewährt die Berechtigung zum Hinzufügen oder Aktualisieren von Tags einer Ressource.	Markieren	device		
			project		
				aws:RequestTag/${TagKey} aws:TagKeys	
UnclaimDevice	Gewährt die Erlaubnis, Beantragung eines Geräts aufzuheben	Read	device*		
UntagResource	Gewährt die Berechtigung zum Entfernen der angegebenen Tags (Metadaten) aus einer Ressource	Markieren	device		
			project		
				aws:TagKeys	
UpdateDeviceState	Gewährt die Berechtigung zum Aktualisieren des Gerätestatus	Write	device*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdatePlacement	Gewährt die Berechtigung zum Aktualisieren einer Plazierung.	Write	project*		
UpdateProject	Projekt aktualisieren	Write	project*		

Von AWS IoT 1-Click definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
device	`arn:${Partition}:iot1click:${Region}:${Account}:devices/${DeviceId}`	aws:ResourceTag/${TagKey}
project	`arn:${Partition}:iot1click:${Region}:${Account}:projects/${ProjectName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS IoT 1-Click

AWS IoT 1-Click definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf den Markierungen, die in der Anforderung übergeben werden.	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf den Markierungen, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert Aktionen basierend auf den Tag-Schlüsseln, die in der Anforderung übergeben werden.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT Analytics

AWS IoT Analytics (Servicepräfix: `iotanalytics`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS IoT Analytics definierte Aktionen
- Von AWS IoT Analytics definierte Ressourcentypen
- Bedingungsschlüssel für AWS IoT Analytics

Von AWS IoT Analytics definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchPutMessage	Schreibt einen Batch Meldungen in den angegebenen Channel	Schreiben	channel*		
CancelPipelineReprocessing	Bricht die erneute Verarbeitung für die angegebene Pipeline ab	Schreiben	pipeline*		
CreateChannel	Erstellt einen Channel	Schreiben	channel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataset	Erstellt ein Dataset	Schreiben	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDatasetContent	Generiert den Inhalt des angegebenen Datensatzes (durch Ausführung der Datensatzaktionen)	Schreiben	dataset*		
CreateDatastore	Erstellt einen Datenspeicher	Schreiben	datastore*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePipeline	Erstellt eine Pipeline	Schreiben	pipeline*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Löscht den angegebenen Channel	Schreiben	channel*		
DeleteDataset	Löscht den angegebenen Datensatz	Schreiben	dataset*		
DeleteDatasetContent	Löscht den Inhalt des angegebenen Datensatzes	Schreiben	dataset*		
DeleteDatastore	Löscht den angegebenen Datenspeicher	Schreiben	datastore*		
DeletePipeline	Löscht die angegebene Pipeline	Schreiben	pipeline*		
DescribeChannel	Beschreibt den angegebenen Channel	Lesen	channel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDataset	Beschreibt den angegebenen Datensatz	Lesen	dataset*		
DescribeDatastore	Beschreibt den angegebenen Datenspeicher	Lesen	datastore*		
DescribeLoggingOptions	Beschreibt die Protokollierungsoptionen für das Konto	Lesen			
DescribePipeline	Beschreibt die angegebene Pipeline	Lesen	pipeline*		
GetDatasetContent	Ruft den Inhalt des angegebenen Datensatzes ab	Lesen	dataset*		
ListChannels	Listet die Channels für das Konto auf	Auflisten			
ListDatasetContents	Listet Informationen zu Datensatzinhalten auf, die erstellt wurden	Auflisten	dataset*		
ListDatasets	Listet die Datensätze für das Konto auf	Auflisten			
ListDatastores	Listet die Datenspeicher für das Konto auf	Auflisten			
ListPipelines	Listet die Pipelines für das Konto auf	Auflisten			
ListTagsForResource		Lesen	channel		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Listet die Tags (Metadaten) auf, die Sie der Ressource zugewiesen haben		dataset		
			datastore		
			pipeline		
PutLoggingOptions	Legt Protokollierungsoptionen für das Konto fest	Schreiben			
RunPipelineActivity	Führt die angegebene Pipeline-Aktivität aus	Lesen			
SampleChannelData	Tastet die Daten im angegebenen Channel ab	Lesen	channel*		
StartPipelineReprocessing	Startet die erneute Verarbeitung für die angegebene Pipeline	Schreiben	pipeline*		
TagResource	Fügt die Tags der angegebenen Ressource hinzu oder ändert sie. Tags sind Metadaten, die zur Verwaltung einer Ressource verwendet werden können.	Markierung	channel		
			dataset		
			datastore		
			pipeline		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UntagResource	Entfernt die angegebenen Tags (Metadaten) von der Ressource	Markierung	channel		
			dataset		
			datastore		
			pipeline		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateChannel	Aktualisiert den angegebenen Channel	Schreiben	channel*		
UpdateDataset	Aktualisiert den angegebenen Datensatz	Schreiben	dataset*		
UpdateDatastore	Aktualisiert den angegebenen Datenspeicher	Schreiben	datastore*		
UpdatePipeline	Aktualisiert die angegebene Pipeline	Schreiben	pipeline*		

Von AWS IoT Analytics definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
channel	`arn:${Partition}:iotanalytics:${Region}:${Account}:channel/${ChannelName}`	aws:RequestTag/${TagKey} aws:TagKeys iotanalytics:ResourceTag/${TagKey}
dataset	`arn:${Partition}:iotanalytics:${Region}:${Account}:dataset/${DatasetName}`	aws:RequestTag/${TagKey} aws:TagKeys iotanalytics:ResourceTag/${TagKey}
datastore	`arn:${Partition}:iotanalytics:${Region}:${Account}:datastore/${DatastoreName}`	aws:RequestTag/${TagKey} aws:TagKeys iotanalytics:ResourceTag/${TagKey}
pipeline	`arn:${Partition}:iotanalytics:${Region}:${Account}:pipeline/${PipelineName}`	aws:RequestTag/${TagKey} aws:TagKeys iotanalytics:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS IoT Analytics

AWS IoT Analytics definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf dem Vorhandensein von Tag-Schlüsseln in der Anforderung	ArrayOfString
iotanalytics:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüsselwertpaaren, die der Ressource angefügt sind	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT Core Device Advisor

AWS IoT Core Device Advisor (Servicepräfix: `iotdeviceadvisor`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS IoT Core Device Advisor definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSuiteDefinition	Gewährt die Berechtigung zum Erstellen einer Suite-Definition	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSuiteDefinition	Gewährt die Berechtigung zum Löschen einer Suite-Definition	Schreiben	Suitedefinition*		
GetEndpoint	Gewährt die Berechtigung zum Abrufen eines Device-Advisor-Endpunkts	Lesen			
GetSuiteDefinition	Gewährt die Berechtigung zum Abrufen einer Suite-Definition	Read	Suitedefinition*		
GetSuiteRun	Gewährt die Berechtigung zum Abrufen einer Suite-Ausführung	Read	Suiterun*		
GetSuiteRunReport	Gewährt die Berechtigung zum Abrufen des Qualifikationsberichts für eine Suite-Ausführung	Read	Suiterun*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListSuiteDefinitions	Gewährt die Berechtigung zum Auflisten von Suite-Definitionen	List			
ListSuiteRuns	Gewährt die Berechtigung zum Auflisten von Suite-Ausführungen	List	Suitedefinition*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags (Metadaten), die einer Ressource zugewiesen sind	Read	Suitedefinition Suiterun		
StartSuiteRun	Gewährt die Berechtigung zum Starten einer Suite-Ausführung	Write		aws:RequestTag/${TagKey} aws:TagKeys	
StopSuiteRun	Gewährt die Berechtigung zum Stoppen einer Suite-Ausführung	Write	Suiterun*		
TagResource	Gewährt die Berechtigung, Tags zur angegebenen Ressource hinzuzufügen oder diese zu ändern. Tags sind Metadaten, die zur Verwaltung einer Ressource verwendet werden können.	Markieren	Suitedefinition Suiterun		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen der angegebenen Tags (Metadaten) aus einer Ressource	Markieren	Suitedefinition		
			Suiterun		
				aws:TagKeys	
UpdateSuiteDefinition	Gewährt die Berechtigung zum Aktualisieren einer Suite-Definition	Write	Suitedefinition*		

Von AWS IoT Core Device Advisor definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Suitedefinition	`arn:${Partition}:iotdeviceadvisor:${Region}:${Account}:suitedefinition/${SuiteDefinitionId}`	aws:ResourceTag/${TagKey}
Suiterun	`arn:${Partition}:iotdeviceadvisor:${Region}:${Account}:suiterun/${SuiteDefinitionId}/${SuiteRunId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS IoT Core Device Advisor

AWS IoT Core Device Advisor definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT Device Tester

AWS IoT Device Tester (Servicepräfix: `iot-device-tester`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS IoT Device Tester definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CheckVersion	Gewährt IoT Device Tester die Berechtigung zum Überprüfen, ob ein bestimmter Satz von Produkt, Test-Suite und Device-Tester-Version kompatibel ist	Lesen			
DownloadTestSuite	Gewährt IoT Device Tester die Berechtigung zum Herunterladen kompatibler Test-Suite-Versionen	Lesen			
LatestIdt	Gewährt IoT Device Tester die Berechtigung zum	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Abrufen von Informationen zur neuesten verfügbaren Version von Device Tester				
SendMetrics	Gewährt IoT Device Tester die Berechtigung zum Senden von Nutzungsmetriken in Ihrem Namen	Schreiben			
Supported Version	Gewährt IoT Device Tester die Berechtigung zum Abrufen einer Liste der unterstützten Produkte und Test-Suite-Versionen	Lesen			

Vom AWS IoT Device Tester definierte Ressourcentypen

AWS IoT Device Tester unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf AWS IoT Device Tester zu ermöglichen, geben Sie in Ihrer Richtlinie `"Resource": "*"` an.

Bedingungsschlüssel für AWS IoT Device Tester

IoT Device Tester besitzt keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT Events

AWS IoT Events (Servicepräfix: `iotevents`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS IoT Events definierte Aktionen
- Von AWS IoT Events definierte Ressourcentypen
- Bedingungsschlüssel für AWS IoT Events

Von AWS IoT Events definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchAcknowledgeAlarm	Gewährt die Berechtigung zum Senden einer oder mehrerer Anforderungen für Bestätigungsaktionen an AWS IoT Events	Schreiben	alarmModel*		
BatchDeleteDetector	Erteilt die Berechtigung zum Löschen einer Detektor-Instance im AWS-IoT-Events-System	Schreiben	detectorModel*		
BatchDisableAlarm	Gewährt die Berechtigung zum Deaktivieren einer oder mehrerer Alarm-Instances	Write	alarmModel*		
BatchEnableAlarm	Gewährt die Berechtigung zum Aktivieren einer oder mehrerer Alarm-Instances	Write	alarmModel*		
BatchPutMessage	Gewährt die Berechtigung zum Senden einer Reihe von	Write	input*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Nachrichten an das AWS IoT-Events-System				
BatchResetAlarm	Gewährt die Berechtigung zum Zurücksetzen einer oder mehrerer Alarm-Instances	Write	alarmModel*		
BatchSnoozeAlarm	Gewährt die Berechtigung, eine oder mehrere Alarm-Instances in den Schlummermodus zu versetzen	Write	alarmModel*		
BatchUpdateDetector	Gewährt die Berechtigung zum Aktualisieren einer Detektor-Instance im AWS IoT-Events-System	Write	detectorModel*		
CreateAlarmModel	Gewährt die Berechtigung zum Erstellen eines Alarmmodells zur Überwachung eines AWS IoT-Events-Eingabeattributs oder einer AWS-IoT-SiteWise-Komponenteneigenschaft	Write	alarmModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDetectorModel	Gewährt die Berechtigung zum Erstellen eines Detektormodells zur Überwachung eines AWS IoT-Events-Eingabeattributs	Write	detectorModel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInput	Gewährt die Berechtigung zum Erstellen einer Eingabe in IotEvents	Write	input*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAlarmModel	Gewährt die Berechtigung zum Löschen eines Alarmmodells	Write	alarmModel*		
DeleteDetectorModel	Gewährt die Berechtigung zum Löschen eines Detektormodells	Write	detectorModel*		
DeleteInput	Gewährt die Berechtigung zum Löschen einer Eingabe.	Write	input*		
DescribeAlarm	Gewährt die Berechtigung zum Abrufen von Informationen über eine Alarm-Instance	Read	alarmModel*		
DescribeAlarmModel	Gewährt die Berechtigung zum Abrufen von Informationen über ein Alarmmodell	Read	alarmModel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDetector	Gewährt die Berechtigung zum Abrufen von Informationen über eine Detektor-Instance	Read	detectorModel*		
DescribeDetectorModel	Gewährt die Berechtigung zum Abrufen von Informationen über ein Detektormodell	Lesen	detectorModel*		
DescribeDetectorModelAnalysis	Gewährt die Berechtigung zum Abrufen von Informationen über ein Detektormodell	Lesen			
DescribeInput	Gewährt die Berechtigung zum Abrufen von Informationen über eine Eingabe	Read	input*		
DescribeLoggingOptions	Gewährt die Berechtigung zum Abrufen der aktuellen Einstellungen der Protokollierungsoptionen in AWS IoT Events	Lesen			
GetDetectorModelAnalysisResults	Gewährt die Berechtigung zum Abrufen der Analyseergebnisse für das Detektormodell	Lesen			
ListAlarmModelVersions	Gewährt die Berechtigung zum Auflisten aller Versionen eines Alarmmodells	List	alarmModel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAlarmModels	Gewährt die Berechtigung zum Auflisten der von Ihnen erstellten Alarmmodelle	List			
ListAlarms	Gewährt die Berechtigung zum Abrufen von Informationen über alle Alarm-Instances nach alarmModel	List	alarmModel*		
ListDetectorModelVersions	Gewährt die Berechtigung zum Auflisten aller Versionen eines Detektormodells	List	detectorModel*		
ListDetectorModels	Gewährt die Berechtigung zum Auflisten der von Ihnen erstellten Detektormodelle	List			
ListDetectors	Gewährt die Berechtigung zum Abrufen von Informationen über alle Detektor-Instances nach detectormodel	List	detectorModel*		
ListInputRoutings	Gewährt die Berechtigung zum Auflisten eines oder mehrerer Eingabe-Routings	List			
ListInputs	Gewährt die Berechtigung zum Auflisten der von Ihnen erstellten Eingaben	List			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags (Metadaten), die Sie der Ressource zugewiesen haben	Read	alarmModel		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			detectorModel		
			input		
PutLoggingOptions	Gewährt die Berechtigung zum Festlegen oder Aktualisieren der Protokollierungsoptionen für AWS IoT Events	Schreiben			
StartDetectorModelAnalysis	Gewährt die Berechtigung zum Starten des Anomaliekennungsmodells	Schreiben			
TagResource	Gewährt die Berechtigung zum Hinzufügen oder Ändern der Tags der angegebenen Ressource. Tags sind Metadaten, die zur Verwaltung einer Ressource verwendet werden können.	Markieren	alarmModel		
			detectorModel		
			input		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung, die angegebenen Tags (Metadaten) aus der Ressource zu entfernen	Markieren	alarmModel		
			detectorModel		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			input		
				aws:TagKeys	
UpdateAlarmModel	Gewährt die Berechtigung zum Aktualisieren eines Alarmmodells	Write	alarmModel*		
UpdateDetectorModel	Gewährt die Berechtigung zum Aktualisieren eines Detektormodells	Write	detectorModel*		
UpdateInput	Gewährt die Berechtigung zum Aktualisieren einer Eingabe.	Write	input*		
UpdateInputRouting	Gewährt die Berechtigung zum Aktualisieren des Eingabe-Routings	Write	input*		

Von AWS IoT Events definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
detectorModel	`arn:${Partition}:iotevents:${Region}:${Account}:detectorModel/${DetectorModelName}`	aws:ResourceTag/${TagKey}
alarmModel	`arn:${Partition}:iotevents:${Region}:${Account}:alarmModel/${AlarmModelName}`	aws:ResourceTag/${TagKey}
input	`arn:${Partition}:iotevents:${Region}:${Account}:input/${InputName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS IoT Events

AWS IoT Events definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tag-Schlüssel-Wert-Paare in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff über die Tags, die an die Ressource angehängt sind.	Zeichenfolge
aws:TagKeys	Filtert Aktionen nach den Tag-Schlüsseln in der Anforderung	ArrayOfString

Bedingungsschlüssel	Beschreibung	Typ
iotevents:keyValue	Filtert den Zugriff nach der instanceId (Schlüsselwert) der Nachricht	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT Fleet Hub for Device Management

AWS IoT Fleet Hub for Device Management (Servicepräfix: `iotfleethub`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS IoT Fleet Hub for Device Management definierte Aktionen
- Von AWS IoT Fleet Hub for Device Management definierte Ressourcentypen
- Bedingungsschlüssel für AWS IoT Fleet Hub for Device Management

Von AWS IoT Fleet Hub for Device Management definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateApplication	Gewährt die Berechtigung zum Erstellen einer Anwendung	Write		aws:RequestTag/${TagKey}	sso:CreateManagedApplicationInstance

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	sso:DescribeRegisteredRegions
DeleteApplication	Gewährt die Berechtigung zum Löschen einer Anwendung	Write	application*		sso:DeleteManagedApplicationInstance
DescribeApplication	Gewährt die Berechtigung zum Beschreiben einer Anwendung	Read	application*		
ListApplications	Gewährt die Berechtigung zum Auflisten aller Anwendungen	List			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten aller Tags für eine Ressource	Read	application		
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren	application		
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Markieren	application		
				aws:TagKeys	
UpdateApplication	Gewährt die Berechtigung zum Aktualisieren einer Anwendung	Write	application*		

Von AWS IoT Fleet Hub for Device Management definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
application	`arn:${Partition}:iotfleethub:${Region}:${Account}:application/${ApplicationId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS IoT Fleet Hub for Device Management

AWS IoT Fleet Hub for Device Management definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet

wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tag-Schlüssel-Wert-Paare in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff über die Tags, die an die Ressource angehängt sind.	Zeichenfolge
aws:TagKeys	Filtert Aktionen nach den Tag-Schlüsseln in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT FleetWise

AWS IoT FleetWise (Servicepräfix: `iotfleetwise`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS IoT FleetWise definierte Aktionen
- Von AWS IoT FleetWise definierte Ressourcentypen
- Bedingungsschlüssel für AWS IoT FleetWise

Von AWS IoT FleetWise definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateVehicleFleet	Gewährt die Berechtigung, das angegebene Fahrzeug einer Flotte zuzuordnen	Schreiben	fleet*		
			vehicle*		
BatchCreateVehicle	Gewährt die Berechtigung zum Erstellen eines Fahrzeug-Batches	Schreiben	decodermanifest*		iot:CreateThing iot:DescribeThing
			modelmanifest*		
			vehicle*		
				aws:RequestTag/${TagKey} aws:TagKeys	
BatchUpdateVehicle	Gewährt die Berechtigung zum Aktualisieren eines Fahrzeug-Batches	Schreiben	vehicle*		
			decodermanifest		
			modelmanifest		
				iotfleetwise:UpdateToModelM	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				anifestArn iotfleetwise:UpdateToDecoderManifestArn	
CreateCampaign	Gewährt die Berechtigung zum Erstellen einer Kampagne	Schreiben	campaign*		
			fleet*		
			signalcatalog*		
			vehicle*		
				aws:RequestTag/${TagKey} aws:TagKeys iotfleetwise:DestinationArn	
CreateDecoderManifest	Gewährt die Berechtigung zum Erstellen eines Decoder-Manifests für ein vorhandenes Modell	Schreiben	decodermanifest*		
			modelmanifest*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFleet	Gewährt die Berechtigung zum Erstellen einer Flotte	Schreiben	fleet*		
			signalcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelManifest	Gewährt die Berechtigung zum Erstellen einer Muster-Manifest-Definition	Schreiben	modelmanifest*		
			signalcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSignalCatalog	Gewährt die Berechtigung zum Erstellen eines Signalkatalogs	Schreiben	signalcatalog*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVehicle	Gewährt die Berechtigung zum Erstellen eines Fahrzeugs	Schreiben	decodermanifest*		iot:CreateThing iot:DescribeThing
			modelmanifest*		
			vehicle*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCampaign	Gewährt die Berechtigung zum Löschen einer Kampagne	Schreiben	campaign*		
DeleteDecoderManifest	Gewährt die Berechtigung zum Löschen des angegebenen Decoder-Manifests	Schreiben	decodermanifest*		
DeleteFleet	Gewährt die Berechtigung zum Löschen einer Flotte	Schreiben	fleet*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteModelManifest	Gewährt die Berechtigung zum Löschen des angegebenen Modellmanifests	Schreiben	modelmanifest*		
DeleteSignalCatalog	Gewährt die Berechtigung zum Löschen eines bestimmten Signalkatalogs	Schreiben	signalcatalog*		
DeleteVehicle	Gewährt die Berechtigung zum Löschen eines Fahrzeugs	Schreiben	vehicle*		
DisassociateVehicleFleet	Gewährt die Berechtigung zum Trennen eines Fahrzeugs von einer bestehenden Flotte	Schreiben	fleet*		
			vehicle*		
GetCampaign	Gewährt die Berechtigung zum Abrufen von zusammenfassenden Informationen für eine angegebene Kampagne	Lesen	campaign*		
GetDecoderManifest	Gewährt die Berechtigung zum Abrufen von zusammenfassenden Informationen für eine angegebene Decoder-Manifest-Definition	Lesen	decodermanifest*		
GetEncryptionConfiguration	Gewährt die Berechtigung zum Abrufen des KMS-basierten Verschlüsselungsstatus für das AWS-Konto	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetFleet	Gewährt die Berechtigung zum Abrufen von zusammenfassenden Informationen für eine Flotte	Lesen	fleet*		
GetLoggingOptions	Gewährt die Berechtigung zum Abrufen der Protokollierungsoptionen für das AWS-Konto	Lesen			
GetModelManifest	Gewährt die Berechtigung zum Abrufen von zusammenfassenden Informationen für eine angegebene Modellmanifest-Definition	Lesen	modelmanifest*		
GetRegisterAccountStatus	Gewährt die Berechtigung zum Abrufen des Konto-Registrierungsstatus bei IoT FleetWise	Lesen			
GetSignalCatalog	Gewährt die Berechtigung zum Abrufen von zusammenfassenden Informationen für einen bestimmten Signalkatalog	Lesen	signalcatalog*		
GetVehicle	Gewährt die Berechtigung zum Abrufen von zusammenfassenden Informationen für ein Fahrzeug	Lesen	vehicle*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetVehicleStatus	Gewährt die Berechtigung zum Abrufen des Status der Kampagnen, die auf einem bestimmten Fahrzeug ausgeführt werden	Lesen	vehicle*		
ImportDecoderManifest	Gewährt die Berechtigung zum Importieren eines bestehenden Decoder-Manifests	Schreiben	decodermanifest*		
ImportSignalCatalog	Gewährt die Berechtigung zum Erstellen eines Signalkatalogs durch Importieren vorhandener Definitionen	Schreiben	signalcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListCampaigns	Gewährt die Berechtigung zum Auflisten von Kampagnen	Lesen			
ListDecoderManifestNetworkInterfaces	Gewährt die Berechtigung zum Auflisten von Netzwerkschnittstellen, die dem vorhandenen Decoder-Manifest zugeordnet sind	Auflisten	decodermanifest*		
ListDecoderManifestSignals	Gewährt die Berechtigung zum Auflisten von Decoder-Manifest-Signalen	Auflisten	decodermanifest*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDecoderManifests	Gewährt die Berechtigung zum Auflisten aller Decoder-Manifeste mit einem optionalen Filter für das Modellmanifest	Lesen			
ListFleets	Gewährt die Berechtigung zum Auflisten von Flotten	Lesen			
ListFleetsForVehicle	Gewährt die Berechtigung, alle Flotten aufzulisten, denen das angegebene Fahrzeug zugeordnet ist	Lesen	vehicle*		
ListModelManifestNodes	Gewährt die Berechtigung zum Auflisten aller Knoten für das angegebenen Modellmanifest	Auflisten	modelmanifest*		
ListModelManifests	Gewährt die Berechtigung zum Auflisten aller Modellmanifeste mit einem optionalen Filter für den Signalkatalog	Lesen			
ListSignalCatalogNodes	Gewährt die Berechtigung zum Auflisten aller Knoten für einen bestimmten Signalkatalog	Lesen	signalcatalog*		
ListSignalCatalogs	Gewährt die Berechtigung zum Auflisten aller Signalkataloge	Lesen			
ListTagsForResource		Lesen	campaign		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource		decodermanifest		
			fleet		
			modelmanifest		
			signalcatalog		
			vehicle		
ListVehicles	Gewährt die Berechtigung zum Auflisten aller Fahrzeuge, mit einem optionalen Filter für das Modellmanifest	Lesen			
ListVehiclesInFleet	Gewährt die Berechtigung zum Auflisten von Fahrzeugen in der angegebenen Flotte	Lesen	fleet*		
PutEncryptionConfiguration	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren der KMS-basierten Verschlüsselung für das AWS-Konto	Schreiben			
PutLoggingOptions	Gewährt die Berechtigung zum Eingeben der Protokollierungsoptionen für das AWS-Konto	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RegisterAccount	Gewährt die Berechtigung zum Registrieren einer AWS-Konto zu IoT FleetWise	Schreiben			iam:PassRole
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Ressource	Markieren	campaign		
			decodermanifest		
			fleet		
			modelmanifest		
			signalcatalog		
			vehicle		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Ressource	Markierung	campaign		
			decodermanifest		
			fleet		
			modelmanifest		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			signalcatalog		
			vehicle		
				aws:TagKeys	
UpdateCampaign	Gewährt die Berechtigung zum Aktualisieren des Namens einer angegebenen Kampagne	Schreiben	campaign*		
UpdateDecoderManifest	Gewährt die Berechtigung zum Aktualisieren einer Decoder-Manifest-Definition	Schreiben	decodermanifest*		
UpdateFleet	Gewährt die Berechtigung zum Aktualisieren der angegebenen Flotte	Schreiben	fleet*		
UpdateModelManifest	Gewährt die Berechtigung zum Löschen der angegebenen Modellmanifest-Definition	Schreiben	modelmanifest*		
UpdateSignalCatalog	Gewährt die Berechtigung zum Aktualisieren einer bestimmten Signalkatalog-Definition	Schreiben	signalcatalog*		
UpdateVehicle	Gewährt die Berechtigung zum Aktualisieren des Fahrzeugs	Schreiben	vehicle*		
			decodermanifest		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			modelmanifest		
				iotfleetwise:UpdateToModelManifestArn iotfleetwise:UpdateToDecoderManifestArn	

Von AWS IoT FleetWise definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
campaign	`arn:${Partition}:iotfleetwise:${Region}:${Account}:campaign/${CampaignName}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
decodermanifest	arn:${Partition}:iotfleetwise:${Region}:${Account}:decoder-manifest/${Name}	aws:ResourceTag/${TagKey}
fleet	arn:${Partition}:iotfleetwise:${Region}:${Account}:fleet/${FleetId}	aws:ResourceTag/${TagKey}
modelmanifest	arn:${Partition}:iotfleetwise:${Region}:${Account}:model-manifest/${Name}	aws:ResourceTag/${TagKey}
signalcatalog	arn:${Partition}:iotfleetwise:${Region}:${Account}:signal-catalog/${Name}	aws:ResourceTag/${TagKey}
vehicle	arn:${Partition}:iotfleetwise:${Region}:${Account}:vehicle/${VehicleId}	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS IoT FleetWise

AWS IoT FleetWise definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString
iotfleetwise:DestinationArn	Filtert den Zugriff nach Kampagnenziel-ARN, z. B. einem S3-Bucket-ARN oder einem Timestream-ARN	ARN
iotfleetwise:UpdateToDecoderManifestArn	Filtert den Zugriff nach einer Liste von IoT-FleetWise-Decoder-Manifest-ARNs	ARN
iotfleetwise:UpdateToModelManifestArn	Filtert den Zugriff nach einer Liste von IoT-FleetWise-Modellmanifest-ARNs	ARN

Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT Greengrass

AWS IoT Greengrass (Servicepräfix: `greengrass`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS IoT Greengrass definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateRoleToGroup	Gewährt die Berechtigung zum Verknüpfen einer Rolle mit einer Gruppe. Die Berechtigungen der Rolle müssen Greengrass-Core-Lambda-Funktionen und Konnektoren erlauben, Aktionen in anderen AWS-Services auszuführen	Write	group*		
AssociateServiceRoleToAccount	Gewährt die Berechtigung zum Verknüpfen einer Rolle mit Ihrem AWS-Konto. IoT Greengrass verwendet diese Rolle für den Zugriff auf Ihre Lambda-Funktionen und die AWS-IoT-Ressourcen.	Berechtigungsverwaltung			
CreateConnectorDefinition	Gewährt die Berechtigung zum Erstellen einer Konnektordefinition	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateConnectorDefinitionVersion	Gewährt die Berechtigung zum Erstellen einer Version einer vorhandenen Konnektordefinition.	Write	connectorDefinition*		
CreateCoreDefinition	Gewährt die Berechtigung zum Erstellen einer Core-Definition	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCoreDefinitionVersion	Gewährt die Berechtigung zum Erstellen einer Version einer vorhandenen Core-Definition. Greengrass-Gruppen müssen jeweils genau einen Greengrass Core enthalten.	Write	coreDefinition*		
CreateDeployment	Gewährt die Berechtigung zum Erstellen einer Bereitstellung	Write	group*		
CreateDeviceDefinition	Gewährt die Berechtigung zum Erstellen einer Gerätedefinition	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDeviceDefinitionVersion	Gewährt die Berechtigung zum Erstellen einer Version einer vorhandenen Gerätedefinition	Write	deviceDefinition*		
CreateFunctionDefinition	Gewährt die Berechtigung zum Erstellen einer Lambda-Funktion, die in einer Gruppe verwendet werden soll, die eine Liste mit Lambda-Funktionen und deren Konfigurationen enthält	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFunctionDefinitionVersion	Gewährt die Berechtigung zum Erstellen einer Version einer vorhandenen Lambda-Funktionsdefinition	Schreiben	functionDefinition*		
CreateGroup	Gewährt die Berechtigung zum Erstellen einer Gruppe	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGroupCertificateAuthority	Gewährt die Berechtigung zum Erstellen einer CA für die Gruppe oder zum Rotieren der vorhandenen CA	Write	group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateGroupVersion	Gewährt die Berechtigung zum Erstellen einer Version einer Gruppe, die bereits definiert wurde	Write	group*		
CreateLoggerDefinition	Gewährt die Berechtigung zum Erstellen einer Logger-Definition	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLoggerDefinitionVersion	Gewährt die Berechtigung zum Erstellen einer Version einer vorhandenen Logger-Definition	Write	loggerDefinition*		
CreateResourceDefinition	Gewährt die Berechtigung zum Erstellen einer Ressourcendefinition, die eine Liste der in einer Gruppe zu verwenden den Ressourcen enthält	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateResourceDefinitionVersion	Gewährt die Berechtigung zum Erstellen einer Version einer vorhandenen Ressourcendefinition	Write	resourceDefinition*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSoftwareUpdateJob	Gewährt die Berechtigung zum Erstellen eines AWS IoT-Auftrags, der Ihre Greengrass Cores veranlasst, die von ihnen ausgeführte Software zu aktualisieren	Write			
CreateSubscriptionDefinition	Gewährt die Berechtigung zum Erstellen einer Abonnementdefinition	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscriptionDefinitionVersion	Gewährt die Berechtigung zum Erstellen einer Version einer vorhandenen Abonnementdefinition	Write	subscriptionDefinition*		
DeleteConnectorDefinition	Gewährt die Berechtigung zum Löschen einer Konnektordefinition.	Write	connectorDefinition*		
DeleteCoreDefinition	Gewährt die Berechtigung zum Löschen einer Core-Definition. Das Löschen einer Definition, die in einer Bereitstellung derzeit verwendet wird, wirkt sich auf künftige Bereitstellungen aus.	Write	coreDefinition*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteDeviceDefinition	Gewährt die Berechtigung zum Löschen einer Gerätedefinition. Das Löschen einer Definition, die in einer Bereitstellung derzeit verwendet wird, wirkt sich auf künftige Bereitstellungen aus.	Write	deviceDefinition*		
DeleteFunctionDefinition	Gewährt die Berechtigung zum Löschen einer Lambda-Funktionsdefinition. Das Löschen einer Definition, die in einer Bereitstellung derzeit verwendet wird, wirkt sich auf künftige Bereitstellungen aus.	Write	functionDefinition*		
DeleteGroup	Gewährt die Berechtigung zum Löschen einer Gruppe, die derzeit in einer Bereitstellung nicht verwendet wird.	Write	group*		
DeleteLoggerDefinition	Gewährt die Berechtigung zum Löschen einer Logger-Definition. Das Löschen einer Definition, die in einer Bereitstellung derzeit verwendet wird, wirkt sich auf künftige Bereitstellungen aus.	Write	loggerDefinition*		
DeleteResourceDefinition	Gewährt die Berechtigung zum Löschen einer Ressourcendefinition.	Write	resourceDefinition*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteSubscriptionDefinition	Gewährt die Berechtigung zum Löschen einer Abonnementdefinition. Das Löschen einer Definition, die in einer Bereitstellung derzeit verwendet wird, wirkt sich auf künftige Bereitstellungen aus.	Write	subscriptionDefinition*		
DisassociateRoleFromGroup	Gewährt die Berechtigung zum Aufheben der Mapping zwischen Rolle und Gruppe.	Write	group*		
DisassociateServiceRoleFromAccount	Gewährt die Berechtigung zum Aufheben der Mapping zwischen der Servicerolle und einem Konto. Ohne Servicerolle funktionieren Bereitstellungen nicht.	Write			
Discover	Gewährt die Berechtigung zum Abrufen von Informationen, die für die Verbindung mit einem Greengrass-Kern erforderlich sind.	Read	thing*		
GetAssociatedRole	Gewährt die Berechtigung zum Abrufen der Rolle, die einer Gruppe zugeordnet ist.	Read	group*		
GetBulkDeploymentStatus	Gewährt die Berechtigung zum Zurückgeben des Status einer Massenbereitstellung.	Read	bulkDeployment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetConnectivityInfo	Gewährt die Berechtigung zum Abrufen der Verbindungsinformationen für einen Core.	Read	connectivityInfo*		
GetConnectorDefinition	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Konnektordefinition.	Read	connectorDefinition*		
GetConnectorDefinitionVersion	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Konnektordefinitionsversion.	Read	connectorDefinition*		
			connectorDefinitionVersion*		
GetCoreDefinition	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Core-Definition.	Read	coreDefinition*		
GetCoreDefinitionVersion	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Core-Definitionsversion.	Read	coreDefinition*		
			coreDefinitionVersion*		
GetDeploymentStatus	Gewährt die Berechtigung zum Zurückgeben des Status einer Bereitstellung.	Read	deployment*		
			group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDeviceDefinition	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Gerätedefinition.	Read	deviceDefinition*		
GetDeviceDefinitionVersion	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Gerätedefinitionsversion.	Read	deviceDefinition*		
			deviceDefinitionVersion*		
GetFunctionDefinition	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Lambda-Funktionsdefinition, z. B. Erstellungszeit und neueste Version	Read	functionDefinition*		
GetFunctionDefinitionVersion	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Lambda-Funktionsdefinition, z. B. die in der Version enthaltenen Lambda-Funktionen und deren Konfigurationen	Read	functionDefinition*		
			functionDefinitionVersion*		
GetGroup	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Gruppe.	Read	group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetGroupCertificateAuthority	Gewährt die Berechtigung zum Zurückgeben des öffentlichen Schlüssels der CA, die einer Gruppe zugeordnet ist.	Read	certificateAuthority*		
			group*		
GetGroupCertificateConfiguration	Gewährt die Berechtigung zum Abrufen der aktuellen Konfiguration für die CA, die von einer Gruppe verwendet wird.	Read	group*		
GetGroupVersion	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Gruppenversion.	Read	group*		
			groupVersion*		
GetLoggerDefinition	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Logger-Definition.	Read	loggerDefinition*		
GetLoggerDefinitionVersion	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Logger-Definitionsversion.	Read	loggerDefinition*		
			loggerDefinitionVersion*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetResourceDefinition	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Ressourcendefinition, z. B. Erstellungszeit und neueste Version	Read	resourceDefinition*		
GetResourceDefinitionVersion	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Ressourcendefinitionsversion ab, z. B. welche Ressourcen in der Version enthalten sind.	Read	resourceDefinition*		
			resourceDefinitionVersion*		
GetServiceRoleForAccount	Gewährt die Berechtigung zum Abrufen der Servicerolle, die einem Konto zugeordnet ist.	Read			
GetSubscriptionDefinition	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Abonnementdefinition.	Read	subscriptionDefinition*		
GetSubscriptionDefinitionVersion	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Abonnementdefinitionsversion.	Read	subscriptionDefinition*		
			subscriptionDefinitionVersion*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetThingRuntimeConfiguration	Gewährt die Berechtigung zum Abrufen der Laufzeitkonfiguration einer Sache	Read	thingRuntimeConfig*		
ListBulkDeploymentDetailedReports	Gewährt die Berechtigung zum Abrufen eine paginierten Liste der Bereitstellungen, die in einer Massenbereitstellungsproduktion gestartet wurden, sowie ihres aktuellen Bereitstellungsstatus.	Read	bulkDeployment*		
ListBulkDeployments	Gewährt die Berechtigung zum Abrufen einer Liste von Massenbereitstellungen.	List			
ListConnectorDefinitionVersions	Gewährt die Berechtigung zum Auflisten der Versionen einer Konnektordefinition.	List	connectorDefinition*		
ListConnectorDefinitions	Gewährt die Berechtigung zum Abrufen einer Liste der Konnektordefinitionen.	List			
ListCoreDefinitionVersions	Gewährt die Berechtigung zum Auflisten der Versionen einer Core-Definition.	List	coreDefinition*		
ListCoreDefinitions	Gewährt die Berechtigung zum Abrufen einer Liste der Core-Definitionen.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDeployments	Gewährt die Berechtigung zum Abrufen einer Liste aller Bereitstellungen für eine Gruppe.	List	group*		
ListDeviceDefinitionVersions	Gewährt die Berechtigung zum Auflisten der Versionen einer Gerätedefinition.	List	deviceDefinition*		
ListDeviceDefinitions	Gewährt die Berechtigung zum Abrufen einer Liste von Gerätedefinitionen.	List			
ListFunctionDefinitionVersions	Gewährt die Berechtigung zum Auflisten der Versionen einer Lambda-Funktionsdefinition.	List	functionDefinition*		
ListFunctionDefinitions	Gewährt die Berechtigung zum Abrufen einer Liste der Lambda-Funktionsdefinitionen.	List			
ListGroupCertificateAuthorities	Gewährt die Berechtigung zum Abrufen einer Liste der aktuellen CAs für eine Gruppe.	List	group*		
ListGroupVersions	Gewährt die Berechtigung zum Auflisten der Versionen einer Gruppe.	List	group*		
ListGroups	Gewährt die Berechtigung zum Abrufen einer Liste der Gruppen.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListLoggerDefinitionVersions	Gewährt die Berechtigung zum Auflisten der Versionen einer Logger-Definition.	List	loggerDefinition*		
ListLoggerDefinitions	Gewährt die Berechtigung zum Abrufen einer Liste der Logger-Definitionen.	List			
ListResourceDefinitionVersions	Gewährt die Berechtigung zum Auflisten der Versionen einer Ressourcendefinition.	List	resourceDefinition*		
ListResourceDefinitions	Gewährt die Berechtigung zum Abrufen einer Liste der Ressourcendefinitionen.	List			
ListSubscriptionDefinitionVersions	Gewährt die Berechtigung zum Auflisten der Versionen einer Abonnementdefinition.	List	subscriptionDefinition*		
ListSubscriptionDefinitions	Gewährt die Berechtigung zum Abrufen einer Liste der Abonnementdefinitionen.	List			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für eine Ressource	Read	bulkDeployment		
			connectorDefinition		
			coreDefinition		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			deviceDefinition		
			functionDefinition		
			group		
			loggerDefinition		
			resourceDefinition		
			subscriptionDefinition		
				aws:RequestTag/${TagKey} aws:TagKeys	
ResetDeployments	Gewährt die Berechtigung zum Zurücksetzen der Bereitstellungen einer Gruppe.	Write	group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartBulkDeployment	Gewährt die Berechtigung zum Bereitstellen mehrerer Gruppen in einer Produktion.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
StopBulkDeployment	Gewährt die Berechtigung zum Anhalten der Ausführung einer Massenbereitstellung.	Write	bulkDeployment*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Ressource	Markieren	bulkDeployment		
			connectorDefinition		
			coreDefinition		
			deviceDefinition		
			functionDefinition		
			group		
			loggerDefinition		
			resourceDefinition		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			subscriptionDefinition		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Ressource	Markieren	bulkDeployment		
			connectorDefinition		
			coreDefinition		
			deviceDefinition		
			functionDefinition		
			group		
			loggerDefinition		
			resourceDefinition		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			subscriptionDefinition		
				aws:TagKeys	
UpdateConnectivityInfo	Gewährt die Berechtigung zum Aktualisieren der Verbindungsinformationen für einen Greengrass Core. Alle Geräte, die zu der Gruppe gehören, die diesen Core enthält, empfangen diese Informationen, um den Speicherort des Cores ermitteln und eine Verbindung zu diesem herzustellen.	Write	connectivityInfo*		
UpdateConnectorDefinition	Gewährt die Berechtigung zum Aktualisieren einer Konnektordefinition.	Write	connectorDefinition*		
UpdateCoreDefinition	Gewährt die Berechtigung zum Aktualisieren einer Core-Definition.	Write	coreDefinition*		
UpdateDeviceDefinition	Gewährt die Berechtigung zum Aktualisieren einer Gerätedefinition.	Write	deviceDefinition*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateFunctionDefinition	Gewährt die Berechtigung zum Aktualisieren einer Lambda-Funktionsdefinition.	Write	functionDefinition*		
UpdateGroup	Gewährt die Berechtigung zum Aktualisieren einer Gruppe.	Write	group*		
UpdateGroupCertificateConfiguration	Gewährt die Berechtigung zum Aktualisieren der Zertifikatablaufdauer für eine Gruppe.	Write	group*		
UpdateLoggerDefinition	Gewährt die Berechtigung zum Aktualisieren einer Logger-Definition.	Write	loggerDefinition*		
UpdateResourceDefinition	Gewährt die Berechtigung zum Aktualisieren einer Ressourcendefinition.	Write	resourceDefinition*		
UpdateSubscriptionDefinition	Gewährt die Berechtigung zum Aktualisieren einer Abonnementdefinition.	Write	subscriptionDefinition*		
UpdateThingRuntimeConfiguration	Gewährt die Berechtigung zum Aktualisieren der Laufzeitkonfiguration eines Dings	Write	thingRuntimeConfig*		

Von AWS IoT Greengrass definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
connectivityInfo	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/things/${ThingName}/connectivityInfo`	
certificateAuthority	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}/certificateauthorities/${CertificateAuthorityId}`	
deployment	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}/deployments/${DeploymentId}`	
bulkDeployment	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/bulk/deployments/${BulkDeploymentId}`	aws:ResourceTag/${TagKey}
group	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}`	aws:ResourceTag/${TagKey}
groupVersion	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}/versions/${VersionId}`	

Ressourcentypen	ARN	Bedingungsschlüssel
coreDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/cores/${CoreDefinitionId}	aws:ResourceTag/${TagKey}
coreDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/cores/${CoreDefinitionId}/versions/${VersionId}	
deviceDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/devices/${DeviceDefinitionId}	aws:ResourceTag/${TagKey}
deviceDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/devices/${DeviceDefinitionId}/versions/${VersionId}	
functionDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/functions/${FunctionDefinitionId}	aws:ResourceTag/${TagKey}
functionDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/functions/${FunctionDefinitionId}/versions/${VersionId}	
subscriptionDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/subscriptions/${SubscriptionDefinitionId}	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
subscriptionDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/subscriptions/${SubscriptionDefinitionId}/versions/${VersionId}	
loggerDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/loggers/${LoggerDefinitionId}	aws:ResourceTag/${TagKey}
loggerDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/loggers/${LoggerDefinitionId}/versions/${VersionId}	
resourceDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/resources/${ResourceDefinitionId}	aws:ResourceTag/${TagKey}
resourceDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/resources/${ResourceDefinitionId}/versions/${VersionId}	
connectorDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/connectors/${ConnectorDefinitionId}	aws:ResourceTag/${TagKey}
connectorDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/connectors/${ConnectorDefinitionId}/versions/${VersionId}	
thing	arn:${Partition}:iot:${Region}:${Account}:thing/${ThingName}	

Ressourcentypen	ARN	Bedingungsschlüssel
thingRuntimeConfig	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/things/${ThingName}/runtimeconfig`	

Bedingungsschlüssel für AWS IoT Greengrass

AWS IoT Greengrass definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den zulässigen Werten für jedes der obligatorischen Tags	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Tag-Wert, der der Ressource zugeordnet ist	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach dem Vorhandensein verbindlicher Tags in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT Greengrass V2

AWS IoT Greengrass V2 (Servicepräfix: `greengrass`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS IoT Greengrass V2 definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateServiceRoleToAccount	Gewährt die Berechtigung zum Verknüpfen einer Rolle mit Ihrem AWS-Konto. IoT Greengrass verwendet diese Rolle für den Zugriff auf Ihre Lambda-Funktionen und die AWS-IoT-Ressourcen.	Berechtigungsverwaltung			iam:PassRole
BatchAssociateClientDeviceWithCoreDevice	Gewährt die Berechtigung zum Zuordnen einer Liste von Clientgeräten an ein Kerngerät	Schreiben	coreDevice*		
BatchDisassociateClientDevi	Gewährt die Berechtigung zum Trennen einer Liste von Clientgeräten von einem Kerngerät	Schreiben	coreDevice*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ceFromCoreDevice					
CancelDeployment	Gewährt die Berechtigung zum Abbrechen einer Bereitstellung	Write	deployment*		iot:CancelJob iot:DeleteThingShadow iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow iot:UpdateJob iot:UpdateThingShadow
CreateComponentVersion	Gewährt die Berechtigung zum Erstellen einer Komponente	Write	component*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDeployment	Gewährt die Berechtigung zum Erstellen einer Bereitstellung	Write		aws:RequestTag/${TagKey} aws:TagKeys	iot:CancelJob iot:CreateJob iot:DeleteThingShadow iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow iot:UpdateJob iot:UpdateThingShadow
DeleteComponent	Gewährt die Berechtigung zum Löschen einer Komponente	Write	componentVersion*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteCoreDevice	Gewährt die Berechtigung zum Löschen eines AWS-IoT-Greengrass-Core-Geräts, das ein AWS-IoT-Objekt ist. Durch diesen Vorgang wird das Kerngerät aus der Liste der Kerngeräte entfernt. Das AWS-IoT-Objekt wird nicht gelöscht.	Schreiben	coreDevice*		iot:DescribeJobExecution
DeleteDeployment	Gewährt die Berechtigung zum Löschen einer Bereitstellung. Um eine aktive Bereitstellung zu löschen, muss sie zuerst abgebrochen werden	Schreiben	deployment*		iot:DeleteJob
DescribeComponent	Gewährt die Berechtigung zum Abrufen von Metadaten für eine Version einer Komponente	Lesen	componentVersion*		
DisassociateServiceRoleFromAccount	Gewährt die Berechtigung zum Aufheben der Mapping zwischen der Servicerolle und einem Konto. Ohne Servicerolle funktionieren Bereitstellungen nicht.	Schreiben			
GetComponent	Gewährt die Berechtigung zum Abrufen des Rezepts für eine Version einer Komponente	Read	componentVersion*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetComponentVersionArtifact	Gewährt die Berechtigung zum Abrufen der vorsignierten URL zum Download eines Artefakts für öffentliche Komponenten	Lesen	componentVersion*		
GetConnectivityInfo	Gewährt die Berechtigung zum Abrufen der Verbindungsinformationen für ein Greengrass Core Device	Lesen	connectivityInfo*		iot:GetThingShadow
GetCoreDevice	Gewährt die Berechtigung zum Abrufen von Metadaten für ein AWS-IoT-Greengrass-Core-Gerät	Read	coreDevice*		
GetDeployment	Gewährt die Berechtigung zum Abrufen einer Bereitstellung	Lesen	deployment*		iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow
GetServiceRoleForAccount	Gewährt die Berechtigung zum Abrufen der Servicerolle, die einem Konto zugeordnet ist.	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListClientDevicesAssociatedWithCoreDevice	Gewährt die Berechtigung zum Abrufen einer paginierten Liste von Client-Geräten, die einem AWS-IoT-Greengrass-Kerngerät zugeordnet sind	Auflisten	coreDevice*		
ListComponentVersions	Gewährt die Berechtigung zum Abrufen einer paginierten Liste aller Versionen einer Komponente	List	component*		
ListComponents	Gewährt die Berechtigung zum Abrufen einer paginierten Liste mit Komponentenzusammenfassungen	List			
ListCoreDevices	Gewährt die Berechtigung zum Abrufen einer paginierten Liste mit AWS-IoT-Greengrass-Core-Geräten	List			
ListDeployments	Gewährt die Berechtigung zum Abrufen einer paginierten Liste mit Bereitstellungen	List			iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListEffectiveDeployments	Gewährt die Berechtigung zum Abrufen einer paginierten Liste mit Bereitstellungsaufgaben, die AWS IoT Greengrass an AWS-IoT-Greengrass-Core-Geräte sendet	List	coreDevice*		iot:DescribeJob iot:DescribeJobExecution iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow
ListInstalledComponents	Gewährt die Berechtigung zum Abrufen einer paginierten Liste der Komponenten, die auf einem AWS-IoT-Greengrass-Core-Gerät ausgeführt werden	List	coreDevice*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für eine Ressource	Lesen	component		
			componentVersion		
			coreDevice		
			deployment		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
ResolveComponentCandidates	Gewährt die Berechtigung zum Auflisten von Komponenten, die den Anforderungen einer Komponente, Version und Plattform entsprechen	List	componentVersion*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Ressource.	Markieren	component		
			componentVersion		
			coreDevice		
			deployment		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Ressource	Markieren	component		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			componentVersion		
			coreDevice		
			deployment		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateConnectivityInfo	Gewährt die Berechtigung zum Aktualisieren der Verbindungsinformationen für einen Greengrass Core. Alle Geräte, die zu der Gruppe gehören, die diesen Core enthält, empfangen diese Informationen, um den Speicherort des Cores ermitteln und eine Verbindung zu diesem herzustellen.	Schreiben	connectivityInfo*		iot:GetThingShadow iot:UpdateThingShadow

Von AWS IoT Greengrass V2 definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden

können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
connectivityInfo	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/things/${ThingName}/connectivityInfo`	
component	`arn:${Partition}:greengrass:${Region}:${Account}:components:${ComponentName}`	aws:ResourceTag/${TagKey}
componentVersion	`arn:${Partition}:greengrass:${Region}:${Account}:components:${ComponentName}:versions:${ComponentVersion}`	aws:ResourceTag/${TagKey}
coreDevice	`arn:${Partition}:greengrass:${Region}:${Account}:coreDevices:${CoreDeviceThingName}`	aws:ResourceTag/${TagKey}
deployment	`arn:${Partition}:greengrass:${Region}:${Account}:deployments:${DeploymentId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS IoT Greengrass V2

AWS IoT Greengrass V2 definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff danach, ob Tag-Schlüssel/Wert-Paare in der Anforderung enthalten sind	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff durch Überprüfung von Tag-Schlüssel/Wert-Paaren, die einer bestimmten Ressource zugeordnet sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch Überprüfung der Tag-Schlüsseln, die in der Anforderung übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT Jobs DataPlane

AWS IoT Jobs DataPlane (Servicepräfix: `iotjobsdata`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS IoT Jobs DataPlane definierte Aktionen
- Von AWS IoT Jobs DataPlane definierte Ressourcentypen
- Bedingungsschlüssel für AWS IoT Jobs DataPlane

Von AWS IoT Jobs DataPlane definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeJobExecution	Gewährt die Berechtigung zum Beschreiben der Aufgabenausführung.	Lesen	thing*		
				iot:JobId	
GetPendingJobExecutions	Gewährt die Berechtigung zum Abrufen der Liste aller Aufträge für ein Objekt, das sich nicht in einem abschließenden Status befinden.	Lesen	thing*		
StartNextPendingJobExecution	Gewährt die Berechtigung zum Abrufen und Starten der nächsten ausstehenden Auftragsausführung für ein Objekt.	Schreiben	thing*		
UpdateJobExecution	Gewährt die Berechtigung zum Aktualisieren einer Auftragsausführung.	Schreiben	thing*		
				iot:JobId	

Von AWS IoT Jobs DataPlane definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
thing	`arn:${Partition}:iot:${Region}:${Account}:thing/${ThingName}`	

Bedingungsschlüssel für AWS IoT Jobs DataPlane

AWS IoT Jobs DataPlane definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
iot:JobId	Filtert den Zugriff von jobId für iotjobsdata:DescribeJobExecution und iotjobsdata:UpdateJobExecution APIs	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT RoboRunner

AWS IoT RoboRunner (Servicepräfix: `iotroborunner`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS IoT Roborunner definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDestination	Gewährt die Berechtigung zum Erstellen eines Ziels	Schreiben	SiteResource*		
CreateSite	Gewährt die Berechtigung zum Erstellen einer Site	Schreiben			iam:CreateServiceLinkedRole
CreateWorker	Gewährt die Berechtigung zum Erstellen eines Workers	Schreiben	WorkerFleetResource*		
CreateWorkerFleet	Gewährt die Berechtigung zum Erstellen einer Worker-Flotte	Schreiben	SiteResource*		
DeleteDestination	Gewährt die Berechtigung zum Löschen eines Ziels	Schreiben	DestinationResource*		
DeleteSite	Gewährt die Berechtigung zum Löschen einer Website	Schreiben	SiteResource*		
DeleteWorker	Gewährt die Berechtigung zum Löschen eines Workers	Schreiben	WorkerResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteWorkerFleet	Gewährt die Berechtigung zum Löschen einer Worker-Flotte	Schreiben	WorkerFleetResource*		
GetDestination	Gewährt die Berechtigung zum Abrufen eines Ziels	Lesen	DestinationResource*		
GetSite	Gewährt die Berechtigung zum Abrufen einer Site	Lesen	SiteResource*		
GetWorker	Gewährt Berechtigungen zum Abrufen eines Workers	Lesen	WorkerResource*		
GetWorkerFleet	Gewährt Berechtigungen zum Abrufen einer Worker-Flotte	Lesen	WorkerFleetResource*		
ListDestinations	Gewährt die Berechtigung zum Auflisten von Zielen	Lesen	SiteResource*		
ListSites	Gewährt die Berechtigung zum Auflisten von Sites	Lesen			
ListWorkerFleets	Gewährt die Berechtigung zum Auflisten von Worker-Flotten	Lesen	SiteResource*		
ListWorkers	Gewährt die Berechtigung zum Auflisten von Workers	Lesen	SiteResource*		
UpdateDestination	Gewährt die Berechtigung zum Aktualisieren eines Ziels	Schreiben	DestinationResource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateSite	Gewährt die Berechtigung, eine Website zu aktualisieren	Schreiben	SiteResource*		
UpdateWorker	Gewährt die Berechtigung zum Aktualisieren eines Workers	Schreiben	WorkerResource*		
UpdateWorkerFleet	Gewährt die Berechtigung zum Aktualisieren einer Worker-Flotte	Schreiben	WorkerFleetResource*		

Von AWS IoT RoboRunner definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
DestinationResource	`arn:${Partition}:iotroborunner:${Region}:${Account}:site/${SiteId}/destination/${DestinationId}`	iotroborunner:DestinationResourceId
SiteResource	`arn:${Partition}:iotroborunner:${Region}:${Account}:site/${SiteId}`	iotroborunner:SiteResourceId

Ressourcentypen	ARN	Bedingungsschlüssel
WorkerFleetResource	`arn:${Partition}:iotroborunner:${Region}:${Account}:site/${SiteId}/worker-fleet/${WorkerFleetId}`	iotroborunner:WorkerFleetResourceId
WorkerResource	`arn:${Partition}:iotroborunner:${Region}:${Account}:site/${SiteId}/worker-fleet/${WorkerFleetId}/worker/${WorkerId}`	iotroborunner:WorkerResourceId

Bedingungsschlüssel für AWS IoT RoboRunner

AWS IoT RoboRunner definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
iotroborunner:DestinationResourceId	Filtert den Zugriff nach Kennung des Ziels	Zeichenfolge
iotroborunner:SiteResourceId	Filtert den Zugriff nach der Kennung der Site	Zeichenfolge
iotroborunner:Work	Filtert den Zugriff nach der Kennung der Worker-Flotte	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
erFleetResourceId		
iotroborunner:WorkerResourceId	Filtert den Zugriff nach der Kennung des Workers	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT SiteWise

AWS IoT SiteWise (Servicepräfix: `iotsitewise`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS IoT SiteWise definierte Aktionen
- Von AWS IoT SiteWise definierte Ressourcentypen
- Bedingungsschlüssel für AWS IoT SiteWise

Von AWS IoT SiteWise definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Associate Assets	Gewährt die Berechtigung zur Zuordnung einer untergeordneten Komponente zu einer	Schreiben	asset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	übergeordneten Komponente in der Hierarchie				
AssociateTimeSeriesToAssetProperty	Gewährt die Berechtigung zum Zuordnen einer Zeitreihe mit einer Komponente	Schreiben	asset*		
			time-series*		
BatchAssociateProjectAssets	Gewährt die Berechtigung, zur Mapping einer Komponente zu einem Projekt	Write	project*		
BatchDisassociateProjectAssets	Gewährt die Berechtigung zur Aufhebung der Mapping von Assets zu einem bestimmten Projekt	Schreiben	project*		
BatchGetAssetPropertyAggregates	Gewährt die Berechtigung zum Abrufen berechneter Aggregate für mehrere Komponenteneigenschaften	Lesen	asset		
			time-series		
BatchGetAssetPropertyValue	Gewährt die Berechtigung zum Abrufen des neuesten Werts für mehrere Komponenteneigenschaften	Lesen	asset		
			time-series		
BatchGetAssetPropertyValueHistory	Gewährt die Berechtigung zum Abrufen des Wertverlaufs für mehrere Komponenteneigenschaften	Lesen	asset		
			time-series		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchPutAssetPropertyValue	Gewährt die Berechtigung zum Setzen von Eigenschaftswerten für Komponenteneigenschaften	Write	asset		
			time-series		
CreateAccessPolicy	Gewährt die Berechtigung zum Erstellen einer Zugriffsrichtlinie für ein bestimmtes Portal oder ein Projekt	Write	portal		
			project		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAsset	Gewährt die Berechtigung zum Erstellen einer Komponente aus einem Komponentenmodell	Write	asset-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssetModel	Gewährt die Berechtigung zum Erstellen eines Komponentenmodells	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAssetModelCompositeModel	Gewährt die Berechtigung zum Erstellen eines Komponentenmodells (Verbundmodell) innerhalb eines Komponentenmodells	Schreiben	asset-model*		
CreateBulkImportJob	Gewährt die Berechtigung zum Erstellen einer Bulk-Importaufgabe	Schreiben			
CreateDashboard	Gewährt die Berechtigung zum Erstellen eines Dashboards in einem Projekt	Write	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateGateway	Gewährt die Berechtigung zum Erstellen eines Gateways	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreatePortal	Gewährt die Berechtigung zum Erstellen eines Portals	Write		aws:RequestTag/${TagKey} aws:TagKeys	sso:CreateManagedApplicationInstance sso:DescribeRegisteredRegions
CreateProject	Gewährt die Berechtigung zum Erstellen eines Projekts in einem Portal	Write	portal*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessPolicy	Gewährt die Berechtigung zum Löschen einer Zugriffsrichtlinie	Write	access-policy*		
DeleteAsset	Gewährt die Berechtigung zum Löschen einer Komponente	Write	asset*		
DeleteAssetModel	Gewährt die Berechtigung zum Löschen eines Komponentenmodells	Schreiben	asset-model*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteAssetModelCompositeModel	Gewährt die Berechtigung zum Löschen eines Komponentenmodells (Verbundmodell)	Schreiben	asset-model*		
DeleteDashboard	Gewährt die Berechtigung zum Löschen eines Dashboards	Write	dashboard*		
DeleteGateway	Gewährt die Berechtigung zum Löschen eines Gateways	Write	gateway*		
DeletePortal	Gewährt die Berechtigung zum Löschen eines Portals	Write	portal*		sso:DeleteManagedApplicationInstance
DeleteProject	Gewährt die Berechtigung zum Löschen eines Projekts	Schreiben	project*		
DeleteTimeSeries	Gewährt die Berechtigung zum Löschen einer Zeitreihe	Schreiben	asset time-series		
DescribeAccessPolicy	Gewährt die Berechtigung zum Beschreiben einer Zugriffsrichtlinie	Lesen	access-policy*		
DescribeAction	Gewährt die Berechtigung zum Beschreiben von Aktionen	Lesen	asset		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeAsset	Gewährt die Berechtigung zum beschreiben einer Komponente	Lesen	asset*		
DescribeAssetCompositeModel	Gewährt die Berechtigung zum Beschreiben eines Komponentenmodells (Verbundmodell)	Lesen	asset*		
DescribeAssetModel	Gewährt die Berechtigung zum Beschreiben eines Komponentenmodells	Lesen	asset-model*		
DescribeAssetModelCompositeModel	Gewährt die Berechtigung zum Beschreiben eines Komponentenmodells (Verbundmodell)	Lesen	asset-model*		
DescribeAssetProperty	Gewährt die Berechtigung zum Beschreiben einer Asset-Eigenschaft	Lesen	asset*		
DescribeBulkImportJob	Gewährt die Berechtigung zum Beschreiben einer Bulk-Importaufgabe	Lesen			
DescribeDashboard	Gewährt die Berechtigung zur Beschreibung eines Dashboards	Read	dashboard*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDefaultEncryptionConfiguration	Gewährt die Berechtigung zum Beschreiben der Standardverschlüsselungskonfiguration für das AWS-Konto	Read			
DescribeGateway	Gewährt die Berechtigung zum Beschreiben eines Gateways	Read	gateway*		
DescribeGatewayCapabilityConfiguration	Gewährt die Berechtigung zum Beschreiben einer Funktionskonfiguration für ein Gateway	Read	gateway*		
DescribeLoggingOptions	Gewährt die Berechtigung zum Beschreiben der Protokollierungsoptionen für das AWS-Konto	Read			
DescribePortal	Gewährt die Berechtigung zum Beschreiben eines Portals	Read	portal*		
DescribeProject	Gewährt die Berechtigung zum Beschreiben eines Projekts	Lesen	project*		
DescribeStorageConfiguration	Gewährt die Berechtigung zum Beschreiben der Standardverschlüsselungskonfiguration für das AWS-Konto	Lesen			
DescribeTimeSeries		Lesen	asset		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Gewährt die Berechtigung zum Beschreiben einer Zeitreihe		time-series		
				aws:RequestTag/${TagKey} aws:TagKeys	
DisassociateAssets	Gewährt die Berechtigung zum Aufheben der Mapping einer untergeordneten Komponente zu einer übergeordneten Komponente in einer Hierarchie	Schreiben	asset*		
DisassociateTimeSeriesFromAssetProperty	Gewährt die Berechtigung zum Aufheben der Zuordnung einer Zeitreihe mit einer Komponente	Schreiben	asset*		
			time-series*		
EnableSiteWiseIntegration [nur Berechtigung]	Gewährt die Berechtigung, IoT SiteWise in andere Dienste integrieren zu lassen	Schreiben			
ExecuteAction	Gewährt die Berechtigung zum Ausführen von Aktionen	Schreiben	asset		
ExecuteQuery	Gewährt die Berechtigung zum Ausführen einer Abfrage	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAssetPropertyAggregates	Gewährt die Berechtigung zum Abrufen berechneter Aggregate für eine Komponenteneigenschaft	Read	asset		
			time-series		
GetAssetPropertyValue	Gewährt die Berechtigung zum Abrufen des neuesten Werts für eine Komponenteneigenschaft	Read	asset		
			time-series		
GetAssetPropertyValueHistory	Gewährt die Berechtigung zum Abrufen der Werthistorie für eine Komponenteneigenschaft	Lesen	asset		
			time-series		
GetInterpolatedAssetPropertyValues	Gewährt die Berechtigung zum Abrufen des neuesten Werts für eine Komponenteneigenschaft	Lesen	asset		
			time-series		
ListAccessPolicies	Gewährt die Berechtigung zum Auflisten aller Zugriffsrichtlinien für eine Identität oder eine Ressource	Auflisten	portal		
			project		
ListActions	Gewährt die Berechtigung zum Auflisten aller Aktionen	Auflisten	asset		
ListAssetModelCompositeModels	Gewährt die Berechtigung zum Auflisten aller Komponentenmodelle (Verbundmodelle)	Auflisten	asset-model*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAssetModelProperties	Gewährt die Berechtigung zum Auflisten von Komponentenmodelleigenschaften	Auflisten	asset-model*		
ListAssetModels	Gewährt die Berechtigung zum Auflisten aller Komponentenmodelle	Auflisten			
ListAssetProperties	Gewährt die Berechtigung zum Auflisten von Komponenteneigenschaften	Auflisten	asset*		
ListAssetRelationships	Gewährt die Berechtigung zum Auflisten des Komponentenbeziehungsdiagramms für eine Komponente	List	asset*		
ListAssets	Gewährt die Berechtigung zum Auflisten aller Komponenten	Auflisten	asset-model		
ListAssociatedAssets	Gewährt die Berechtigung zum Auflisten aller Komponenten, die einer Komponente durch eine Hierarchie zugeordnet sind	Auflisten	asset*		
ListBulkImportJobs	Gewährt die Berechtigung zum Auflisten von Bulk-Importaufgaben	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListCompositionRelationships	Gewährt die Berechtigung zum Auflisten aller Beziehungen von Komponentenmodellen (Verbundmodelle)	Auflisten	asset-model*		
ListDashboards	Gewährt die Berechtigung zum Auflisten aller Dashboards in einem Projekt	List	project*		
ListGateways	Gewährt die Berechtigung zum Auflisten aller Gateways	List			
ListPortals	Gewährt die Berechtigung zum Auflisten aller Portale	List			
ListProjectAssets	Gewährt die Berechtigung zum Auflisten aller Komponenten, die einem Projekt zugeordnet sind	List	project*		
ListProjects	Gewährt die Berechtigung zum Auflisten aller Projekte in einem Portal	List	portal*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten aller Tags für eine Ressource	Lesen	access-policy		
			asset		
			asset-model		
			dashboard		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			gateway		
			portal		
			project		
			time-series		
				aws:ResourceTag/${TagKey}	
ListTimeSeries	Gewährt die Berechtigung zum Auflisten von Zeitreihen	Auflisten	asset		
PutDefaultEncryptionConfiguration	Gewährt die Berechtigung zum Festlegen der Standardverschlüsselungskonfiguration für das AWS-Konto	Write			
PutLoggingOptions	Gewährt die Berechtigung zum Festlegen der Protokollierungsoptionen für das AWS-Konto	Schreiben			
PutStorageConfiguration	Gewährt die Berechtigung zum Festlegen einer Speicherkonfiguration für dasAWS-Konto	Schreiben			
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren	access-policy		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			asset		
			asset-model		
			dashboard		
			gateway		
			portal		
			project		
			time-series		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Markieren	access-policy		
			asset		
			asset-model		
			dashboard		
			gateway		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			portal		
			project		
			time-series		
				aws:TagKeys	
UpdateAccessPolicy	Gewährt die Berechtigung zum Aktualisieren einer Zugriffsrichtlinie	Write	access-policy*		
UpdateAsset	Gewährt die Berechtigung zum Aktualisieren einer Komponente	Write	asset*		
UpdateAssetModel	Gewährt die Berechtigung zum Aktualisieren eines Komponentenmodells	Schreiben	asset-model*		
UpdateAssetModelCompositeModel	Gewährt die Berechtigung zum Aktualisieren eines Komponentenmodells (Verbundmodell)	Schreiben	asset-model*		
UpdateAssetModelPropertyRouting [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren eines AssetModel-Eigenschafts-Routings	Write	asset-model*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateAssetProperty	Gewährt die Berechtigung zum Aktualisieren einer Komponenteneigenschaft	Write	asset*		
UpdateDashboard	Gewährt die Berechtigung zum Aktualisieren eines Dashboards	Write	dashboard*		
UpdateGateway	Gewährt die Berechtigung zum Aktualisieren eines Gateways	Write	gateway*		
UpdateGatewayCapabilityConfiguration	Gewährt die Berechtigung zum Aktualisieren einer Funktionskonfiguration für ein Gateway	Write	gateway*		
UpdatePortal	Gewährt die Berechtigung zum Aktualisieren eines Portals	Write	portal*		
UpdateProject	Gewährt die Berechtigung zum Aktualisieren eines Projekts	Write	project*		

Von AWS IoT SiteWise definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
asset	arn:${Partition}:iotsitewise:${Region}:${Account}:asset/${AssetId}	aws:ResourceTag/${TagKey}
asset-model	arn:${Partition}:iotsitewise:${Region}:${Account}:asset-model/${AssetModelId}	aws:ResourceTag/${TagKey}
time-series	arn:${Partition}:iotsitewise:${Region}:${Account}:time-series/${TimeSeriesId}	aws:ResourceTag/${TagKey}
gateway	arn:${Partition}:iotsitewise:${Region}:${Account}:gateway/${GatewayId}	aws:ResourceTag/${TagKey}
portal	arn:${Partition}:iotsitewise:${Region}:${Account}:portal/${PortalId}	aws:ResourceTag/${TagKey}
project	arn:${Partition}:iotsitewise:${Region}:${Account}:project/${ProjectId}	aws:ResourceTag/${TagKey}
dashboard	arn:${Partition}:iotsitewise:${Region}:${Account}:dashboard/${DashboardId}	aws:ResourceTag/${TagKey}
access-policy	arn:${Partition}:iotsitewise:${Region}:${Account}:access-policy/${AccessPolicyId}	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS IoT SiteWise

AWS IoT SiteWise definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tag-Schlüssel-Wert-Paare in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff über die Tags, die an die Ressource angehängt sind.	Zeichenfolge
aws:TagKeys	Filtert Aktionen nach den Tag-Schlüsseln in der Anforderung	ArrayOfString
iotsitewise:assetHierarchyPath	Filtert den Zugriff nach einem Komponentenhierarchiepfad, bei dem es sich um die Zeichenfolge der Komponenten-IDs in der Komponentenhierarchie handelt, die jeweils durch einen Schrägstrich getrennt sind.	Zeichenfolge
iotsitewise:childAssetId	Filtert den Zugriff nach der ID einer untergeordneten Komponente, die einer übergeordneten Komponente zugeordnet ist	Zeichenfolge
iotsitewise:group	Filtert den Zugriff nach der ID einer AWS-Single-Sign-On-Gruppe	Zeichenfolge
iotsitewise:iam	Filtert den Zugriff nach der ID einer AWS-IAM-Identität	Zeichenfolge
iotsitewise:isAssociatedWithAssetProperty	Filtert den Zugriff nach Datenströmen, die mit Komponenten-Eigenschaften verknüpft sind oder nicht	Zeichenfolge
iotsitewise:portal	Filtert den Zugriff anhand der ID eines Portals	Zeichenfolge
iotsitewise:project	Filtert den Zugriff anhand der ID eines Projekts	String

Bedingungsschlüssel	Beschreibung	Typ
iotsitewise:propertyAlias	Filtert den Zugriff nach dem Eigenschafts-Alias	Zeichenfolge
iotsitewise:propertyId	Filtert den Zugriff nach der ID einer Komponenteneigenschaft	Zeichenfolge
iotsitewise:user	Filtert den Zugriff nach der ID eines AWS-Single-Sign-On-Benutzers	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT TwinMaker

AWS IoT TwinMaker (Servicepräfix: `iottwinmaker`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS IoT TwinMaker definierte Aktionen
- Von AWS IoT TwinMaker definierte Ressourcentypen
- Bedingungsschlüssel für AWS IoT TwinMaker

Von AWS IoT TwinMaker definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchPutPropertyValues	Gewährt die Berechtigung zum Festlegen von Werten für	Schreiben	workspace*		iottwinmaker:GetCo

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	mehrere Zeitreihen-Eigenschaften				mponentType iottwinmaker:GetEntity iottwinmaker:GetWorkspace
			entity		
CancelMetadataTransferJob	Gewährt die Berechtigung zum Abbrechen einer Metadatentransferaufgabe	Schreiben	metadataTransferJob*		
CreateComponentType	Gewährt die Berechtigung zum Erstellen einer componentType	Schreiben	workspace*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEntity	Gewährt die Berechtigung zum Erstellen einer juristischen Stelle	Schreiben	workspace*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMetadataTransferJob	Gewährt die Berechtigung zum Erstellen eines Metadatentransferauftrags	Schreiben			
CreateScene	Gewährt die Berechtigung zum Erstellen einer Szene	Schreiben	workspace*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSyncJob	Gewährt die Berechtigung zum Erstellen eines Synchronisierungsauftrags	Schreiben	workspace*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateWorkspace	Gewährt die Berechtigung zum Erstellen eines Workspace	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteComponentType	Gewährt die Berechtigung zum Löschen einer componentType	Schreiben	componentType*		
			workspace*		
DeleteEntity	Gewährt die Berechtigung zum Löschen einer juristischen Stelle	Schreiben	entity*		
			workspace*		
DeleteScene	Gewährt die Berechtigung zum Löschen einer Szene	Schreiben	scene*		
			workspace*		
DeleteSyncJob	Gewährt die Berechtigung zum Löschen eines Synchronisierungsauftrags	Schreiben	syncJob*		
			workspace*		
DeleteWorkspace	Gewährt die Berechtigung zum Löschen eines Workspace	Schreiben	workspace*		
ExecuteQuery	Gewährt die Berechtigung zum Ausführen einer Abfrage	Lesen	workspace*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetComponentType	Gewährt die Berechtigung zum Abrufen einer component Type	Lesen	componentType*		
			workspace*		
GetEntity	Gewährt die Berechtigung zum Abrufen einer juristischen Stelle	Lesen	entity*		
			workspace*		
GetMetadataTransferJob	Gewährt die Berechtigung zum Abrufen eines Metadaten transferauftrags	Lesen	metadataTransferJob*		
GetPricingPlan	Gewährt die Berechtigung zum Erhalten eines Preisplans	Lesen			
GetPropertyValue	Gewährt die Berechtigung zum Abrufen des Eigenschafts-Werts	Lesen	workspace*		iottwinmaker:GetComponentType iottwinmaker:GetEntity iottwinmaker:GetWorkspace
			componentType		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			entity		
GetPropertyValueHistory	Gewährt die Berechtigung zum Abrufen der Werthistorie für eine Zeitreihe	Lesen	workspace*		iottwinmaker:GetComponentType iottwinmaker:GetEntity iottwinmaker:GetWorkspace
			componentType		
			entity		
GetScene	Gewährt die Berechtigung zum Abrufen einer Szene	Lesen	scene*		
			workspace*		
GetSyncJob	Gewährt die Berechtigung zum Abrufen einer Synchronisationsaufgabe	Lesen	syncJob*		
			workspace*		
GetWorkspace	Gewährt Berechtigungen zum Abrufen eines Workspace	Lesen	workspace*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListComponentTypes	Gewährt die Berechtigung zum Auflisten aller Component Types in einem Workspace	Auflisten	workspace*		
ListComponents	Gewährt die Berechtigung zum Auflisten der Komponenten, die einer Entität zugeordnet sind	Auflisten	entity* workspace*		
ListEntities	Gewährt die Berechtigung zum Auflisten aller juristischer Stellen in einem Workspace	Auflisten	workspace*		
ListMetadataTransferJobs	Gewährt die Berechtigung zum Auflisten aller Metadaten transferaufträge	Auflisten			
ListProperties	Gewährt die Berechtigung zum Auflisten der Eigenschaften einer Entitätskomponente	Auflisten	entity* workspace*		
ListScenes	Gewährt die Berechtigung zum Auflisten aller Szenen in einem Workspace	Auflisten	workspace*		
ListSyncJobs	Gewährt die Berechtigung zum Auflisten von allen Synchronisierungsaufträgen in einem Workspace	Auflisten	workspace*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListSyncResources	Gewährt die Berechtigung zum Auflisten von allen Synchronisierungsressourcen für einen Synchronisierungsauftrag	Auflisten	syncJob*		
			workspace*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten aller Tags für eine Ressource	Auflisten	componentType		
			entity		
			scene		
			syncJob		
			workspace		
				aws:ResourceTag/${TagKey}	
ListWorkspaces	Gewährt die Berechtigung zum Auflisten von Workspaces	Auflisten			
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren	componentType		
			entity		
			scene		
			syncJob		
			workspace		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Tagging	componentType		
			entity		
			scene		
			syncJob		
			workspace		
				aws:TagKeys	
UpdateComponentType	Gewährt die Berechtigung zum Aktualisieren einer componentType	Schreiben	componentType*		
			workspace*		
UpdateEntity	Gewährt die Berechtigung zum Aktualisieren einer juristischen Stelle	Schreiben	entity*		
			workspace*		
UpdatePricingPlan	Gewährt die Berechtigung zum Aktualisieren eines Preisplans	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateScene	Gewährt die Berechtigung zum Aktualisieren einer Szene	Schreiben	scene*		
			workspace*		
UpdateWorkspace	Gewährt die Berechtigung zum Aktualisieren eines Workspace	Schreiben	workspace*		

Von AWS IoT TwinMaker definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
workspace	`arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}`	aws:ResourceTag/${TagKey}
entity	`arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}/entity/${EntityId}`	aws:ResourceTag/${TagKey}
componentType	`arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${Workspace`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
	`Id}/component-type/${ComponentTypeId}`	
scene	`arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}/scene/${SceneId}`	aws:ResourceTag/${TagKey}
syncJob	`arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}/sync-job/${SyncJobId}`	aws:ResourceTag/${TagKey}
metadataTransferJob	`arn:${Partition}:iottwinmaker:${Region}:${Account}:metadata-transfer-job/${MetadataTransferJobId}`	

Bedingungsschlüssel für AWS IoT TwinMaker

AWS IoT TwinMaker definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tag-Schlüssel-Wert-Paare in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff über die Tags, die an die Ressource angehängt sind.	String

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert Aktionen nach den Tag-Schlüsseln in der Anforderung	ArrayOfString
iottwinmaker:destinationType	Filtert den Zugriff nach dem Zieltyp des Metadaten transferauftrags	ArrayOfString
iottwinmaker:linkedServices	Filtert den Zugriff nach dem Workspace, der mit Diensten verknüpft ist	ArrayOfString
iottwinmaker:sourceType	Filtert den Zugriff nach Quelltyp des Metadaten-Übertragungsauftrags	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT Wireless

AWS IoT Wireless (Dienstpräfix:`iotwireless`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS IoT Wireless definierte Aktionen
- Von AWS IoT Wireless definierte Ressourcentypen
- Bedingungsschlüssel für AWS IoT Wireless

Von AWS IoT Wireless definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateAwsAccountWithPartnerAccount	Erteilt die Berechtigung zum Verknüpfen von Partnerkonten mit AWS-Konto	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
AssociateMulticastGroupWithFuotaTask	Erteilt die Erlaubnis zur Verknüpfung MulticastGroup mit FuotaTask	Schreiben	FuotaTask* MulticastGroup*		
AssociateWirelessDeviceWithFuotaTask	Erteilt die Berechtigung zum Zuordnen des drahtlosen Geräts zu FuotaTask	Schreiben	FuotaTask* WirelessDevice*		
AssociateWirelessDeviceWithMulticastGroup	Erteilt die Berechtigung zur Verknüpfung WirelessDevice mit MulticastGroup	Schreiben	MulticastGroup* WirelessDevice*		
AssociateWirelessDeviceWithThing	Erteilt die Erlaubnis, das drahtlose Gerät mit einem AWS IoT-Ding für ein bestimmtes Objekt zu verknüpfen wirelessDeviceId	Schreiben	WirelessDevice* thing*		iot:DescribeThing
AssociateWirelessG	Erteilt die Berechtigung, ein Zertifikat WirelessGateway mit	Schreiben	WirelessGateway*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
atewayWithCertificate	dem IoT Core Identity-Zertifikat zu verknüpfen		cert*		
AssociateWirelessGatewayWithThing	Erteilt die Erlaubnis, das Wireless-Gateway mit einem AWS IoT-Ding für ein bestimmtes Objekt zu verknüpfen wirelessGatewayId	Schreiben	WirelessGateway*		iot:DescribeThing
			thing*		
CancelMulticastGroupSession	Erteilt die Erlaubnis, die MulticastGroup Sitzung abzubrechen	Schreiben	MulticastGroup*		
CreateDestination	Gewährt die Berechtigung zum Erstellen einer Zielressource	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeviceProfile	Erteilt die Berechtigung zum Erstellen einer DeviceProfile Ressource	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFuotaTask	Erteilt die Berechtigung zum Erstellen einer FuotaTask Ressource	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateMulticastGroup	Erteilt die Berechtigung zum Erstellen einer MulticastGroup Ressource	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateNetworkAnalyzerConfiguration	Erteilt die Berechtigung zum Erstellen einer NetworkAnalyzerConfiguration Ressource	Schreiben	MulticastGroup*		
			WirelessDevice*		
			WirelessGateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateServiceProfile	Erteilt die Berechtigung zum Erstellen einer ServiceProfile Ressource	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateWirelessDevice	Erteilt die Erlaubnis, eine WirelessDevice Ressource mit dem angegebenen Ziel zu erstellen	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWirelessGateway	Erteilt die Erlaubnis, eine WirelessGateway Ressource zu erstellen	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWirelessGatewayTask	Erteilt die Berechtigung, eine Aufgabe für eine bestimmte Aufgabe zu erstellen WirelessGateway	Schreiben	WirelessGateway*		
CreateWirelessGatewayTaskDefinition	Erteilt die Berechtigung zum Erstellen einer WirelessGateway Aufgabendefinition	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDestination	Gewährt die Berechtigung zum Löschen eines Ziels	Schreiben	Destination*		
DeleteDeviceProfile	Erteilt die Berechtigung zum Löschen eines DeviceProfile	Schreiben	DeviceProfile*		
DeleteFuotaTask	Erteilt die Erlaubnis zum Löschen von FuotaTask	Schreiben	FuotaTask*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteMulticastGroup	Erteilt die Erlaubnis zum Löschen von MulticastGroup	Schreiben	MulticastGroup*		
DeleteNetworkAnalyzerConfiguration	Erteilt die Erlaubnis zum Löschen von NetworkAnalyzerConfiguration	Schreiben	NetworkAnalyzerConfiguration*		
DeleteQueuedMessages	Erteilt die Erlaubnis zum Löschen QueuedMessages	Schreiben			
DeleteServiceProfile	Erteilt die Erlaubnis zum Löschen eines ServiceProfile	Schreiben	ServiceProfile*		
DeleteWirelessDevice	Erteilt die Erlaubnis zum Löschen eines WirelessDevice	Schreiben	WirelessDevice*		
DeleteWirelessDeviceImportTask	Gewährt die Berechtigung zum Löschen der Importaufgabe für drahtlose Geräte	Schreiben	ImportTask*		
DeleteWirelessGateway	Erteilt die Erlaubnis zum Löschen eines WirelessGateway	Schreiben	WirelessGateway*		
DeleteWirelessGatewayTask	Erteilt die Erlaubnis, eine Aufgabe für eine bestimmte Aufgabe zu löschen WirelessGateway	Schreiben	WirelessGateway*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteWirelessGatewayTaskDefinition	Erteilt die Berechtigung zum Löschen einer WirelessGateway Aufgabendefinition	Schreiben	WirelessGatewayTaskDefinition*		
DeregisterWirelessDevice	Gewährt die Berechtigung zum Aufheben der Registrierung eines drahtlosen Gerät	Schreiben	WirelessDevice*		
DisassociateAwsAccountFromPartnerAccount	Erteilt die Berechtigung, eine Person AWS-Konto von einem Partnerkonto zu trennen	Schreiben	SidewalkAccount*		
DisassociateMulticastGroupFromFuotaTask	Erteilt die Erlaubnis, die Verknüpfung mit dem zu trennen MulticastGroup FuotaTask	Schreiben	FuotaTask*		
			MulticastGroup*		
DisassociateWirelessDeviceFromFuotaTask	Erteilt die Erlaubnis, die Verbindung des drahtlosen Geräts zu trennen FuotaTask	Schreiben	FuotaTask*		
			WirelessDevice*		
DisassociateWirelessDeviceFromMulticastGroup	Erteilt die Erlaubnis, die Verbindung des drahtlosen Geräts zu trennen Multicast Group	Schreiben	MulticastGroup*		
			WirelessDevice*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateWirelessDeviceFromThing	Erteilt die Erlaubnis, ein drahtloses Gerät von einem AWS IoT-Ding zu trennen	Schreiben	WirelessDevice*		iot:DescribeThing
			thing*		
DisassociateWirelessGatewayFromCertificate	Erteilt die Erlaubnis, ein Zertifikat WirelessGateway von einem IoT Core Identity-Zertifikat zu trennen	Schreiben	WirelessGateway*		
			cert*		
DisassociateWirelessGatewayFromThing	Erteilt die Erlaubnis, eine Sache WirelessGateway von einem IoT Core-Ding zu trennen	Schreiben	WirelessGateway*		iot:DescribeThing
			thing*		
GetDestination	Gewährt die Berechtigung zum Abrufen des Ziels	Lesen	Destination*		
GetDeviceProfile	Erteilt die Erlaubnis zum Abrufen der DeviceProfile	Lesen	DeviceProfile*		
GetEventConfigurationByResourceTypes	Gewährt die Berechtigung zum Abrufen von Ereigniskonfiguration nach Ressourcentypen	Lesen			
GetFuotaTask	Erteilt die Erlaubnis zum Abrufen der FuotaTask	Lesen	FuotaTask*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetLogLevelsByResourceTypes	Gewährt die Berechtigung zum Abrufen von Protokollebenen nach Ressourcentypen	Lesen			
GetMetricConfiguration	Erteilt die Berechtigung zum Abrufen der metrischen Konfiguration	Lesen			
GetMetrics	Erteilt die Erlaubnis zum Abrufen von Metriken	Lesen			
GetMulticastGroup	Erteilt die Erlaubnis zum Abrufen der MulticastGroup	Lesen	MulticastGroup*		
GetMulticastGroupSession	Erteilt die Erlaubnis zum Abrufen der MulticastGroup Sitzung	Lesen	MulticastGroup*		
GetNetworkAnalyzerConfiguration	Erteilt die Erlaubnis zum Abrufen der NetworkAnalyzerConfiguration	Lesen	NetworkAnalyzerConfiguration*		
GetPartnerAccount	Erteilt die Erlaubnis, die zugehörige Datei abzurufen PartnerAccount	Lesen	SidewalkAccount*		
GetPosition	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen	WirelessDevice		
			WirelessGateway		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetPositionConfiguration	Gewährt die Berechtigung zum Abrufen der Positionskonfiguration für eine Ressource	Lesen	WirelessDevice		
			WirelessGateway		
GetPositionEstimate	Gewährt die Berechtigung zum Abrufen einer Verwendung	Lesen			
GetResourceEventConfiguration	Gewährt die Berechtigung zum Abrufen einer Ereigniskonfiguration für eine Kennung	Lesen	SidewalkAccount		
			WirelessDevice		
			WirelessGateway		
GetResourceLogLevel	Gewährt die Berechtigung zum Abrufen von Ressourcenprotokollebenen	Lesen	WirelessDevice		
			WirelessGateway		
GetResourcePosition	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen	WirelessDevice		
			WirelessGateway		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetServiceEndpoint	Erteilt die Berechtigung, den kundenkontospezifischen Endpunkt für die CUPS-Protokollverbindung oder die LoRa WAN-Netzwerkserver-Protokollverbindung (LNS) und optional das Server-Vertrauenszertifikat im PEM-Format abzurufen	Lesen			
GetServiceProfile	Erteilt die Erlaubnis zum Abrufen des ServiceProfile	Lesen	ServiceProfile*		
GetWirelessDevice	Erteilt die Erlaubnis zum Abrufen der WirelessDevice	Lesen	WirelessDevice*		
GetWirelessDeviceImportTask	Gewährt die Berechtigung zum Abrufen der Importaufgabe für drahtlose Geräte	Lesen	ImportTask*		
GetWirelessDeviceStatistics	Erteilt die Erlaubnis, Statistikinformationen für eine bestimmte Datei abzurufen WirelessDevice	Lesen	WirelessDevice*		
GetWirelessGateway	Erteilt die Erlaubnis zum Abrufen der WirelessGateway	Lesen	WirelessGateway*		
GetWirelessGatewayCertificate	Erteilt die Berechtigung zum Abrufen der IoT Core Identity-Zertifikat-ID, die dem zugeordnet ist WirelessGateway	Lesen	WirelessGateway*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetWirelessGatewayFirmwareInformation	Erteilt die Erlaubnis zum Abrufen der aktuellen Firmware-Version und anderer Informationen für WirelessGateway	Lesen	WirelessGateway*		
GetWirelessGatewayStatistics	Erteilt die Erlaubnis, Statistikinformationen für eine bestimmte Datei abzurufen WirelessGateway	Lesen	WirelessGateway*		
GetWirelessGatewayTask	Erteilt die Erlaubnis, die Aufgabe für eine bestimmte Aufgabe abzurufen WirelessGateway	Lesen	WirelessGateway*		
GetWirelessGatewayTaskDefinition	Erteilt die Berechtigung zum Abrufen der angegebenen WirelessGateway Aufgabendefinition	Lesen	WirelessGatewayTaskDefinition*		
ListDestinations	Erteilt die Berechtigung, Informationen über verfügbare Ziele aufzulisten, basierend auf AWS-Konto	Lesen			
ListDeviceProfiles	Erteilt die Berechtigung zum Auflisten verfügbarer Informationen auf der DeviceProfiles Grundlage von AWS-Konto	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDevicesForWirelessDeviceImportTask	Erteilt die Berechtigung, Geräteinformationen anhand der Importaufgabe für drahtlose Geräte aufzulisten, basierend auf AWS-Konto	Lesen	ImportTask*		
ListEventConfigurations	Erteilt die Berechtigung, Informationen zu verfügbaren Ereigniskonfigurationen aufzulisten, basierend auf AWS-Konto	Lesen			
ListFuotaTasks	Erteilt die Berechtigung zum Auflisten verfügbarer Informationen auf der FuotaTasks Grundlage von AWS-Konto	Lesen			
ListMulticastGroups	Erteilt die Berechtigung zum Auflisten verfügbarer Informationen auf der MulticastGroups Grundlage von AWS-Konto	Lesen			
ListMulticastGroupsByFuotaTask	Erteilt die Berechtigung zum Auflisten MulticastGroups von verfügbaren Informationen auf der FuotaTask Grundlage von AWS-Konto	Lesen	FuotaTask*		
ListNetworkAnalyzerConfigurations	Erteilt die Berechtigung zum Auflisten verfügbarer Informationen auf der NetworkAnalyzerConfigurations Grundlage von AWS-Konto	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListPartnerAccounts	Gewährt die Berechtigung zum Auflisten der verfügbaren Partnerkonten	Lesen			
ListPositionConfigurations	Erteilt die Berechtigung, Informationen über verfügbare Positionskonfigurationen aufzulisten, basierend auf AWS-Konto	Lesen			
ListQueuedMessages	Gewährt die Berechtigung zum Auflisten von QueuedMessages	Lesen			
ListServiceProfiles	Erteilt die Berechtigung zum Auflisten verfügbarer Informationen auf der ServiceProfiles Grundlage von AWS-Konto	Lesen			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen	Destination		
			DeviceProfile		
			FuotaTask		
			ImportTask		
			MulticastGroup		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			NetworkAnalyzerConfiguration		
			ServiceProfile		
			SidewalkAccount		
			WirelessDevice		
			WirelessGateway		
			WirelessGatewayTaskDefinition		
ListWirelessDeviceImportTasks	Erteilt die Berechtigung, Informationen zu Importaufgaben für drahtlose Geräte aufzulisten, basierend auf AWS-Konto	Lesen			
ListWirelessDevices	Erteilt die Berechtigung zum Auflisten verfügbarer Informationen auf der WirelessDevices Grundlage von AWS-Konto	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListWirelessGatewayTaskDefinitions	Erteilt die Berechtigung zum Auflisten von Informationen verfügbarer WirelessGateway Aufgabendefinitionen auf der Grundlage von AWS-Konto	Lesen			
ListWirelessGateways	Erteilt die Berechtigung zum Auflisten verfügbarer Informationen auf der WirelessGateways Grundlage von AWS-Konto	Lesen			
PutPositionConfiguration	Gewährt die Berechtigung zum Platzieren von Positionskonfigurationen für eine Ressource	Schreiben	WirelessDevice		
			WirelessGateway		
PutResourceLogLevel	Gewährt die Berechtigung zum Speichern von Protokollebenen nach Ressourcenprotokollebenen	Write	WirelessDevice		
			WirelessGateway		
ResetAllResourceLogLevels	Gewährt die Berechtigung zum Zurücksetzen aller Ressourcentypen	Write			
ResetResourceLogLevel	Gewährt die Berechtigung zum Zurücksetzen der Ressourcenprotokollebene	Schreiben	WirelessDevice		
			WirelessGateway		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SendDataToMulticastGroup	Erteilt die Erlaubnis zum Senden von Daten an MulticastGroup	Schreiben	MulticastGroup*		
SendDataToWirelessDevice	Gewährt die Berechtigung zum Senden des entschlüsselten Anwendungsdatenrahmens an das Zielgerät	Schreiben	WirelessDevice*		
StartBulkAssociateWirelessDeviceWithMulticastGroup	Erteilt die Erlaubnis zur Verknüpfung WirelessDevices mit MulticastGroup	Schreiben	MulticastGroup*		
StartBulkDisassociateWirelessDeviceFromMulticastGroup	Erteilt die Erlaubnis, die Verknüpfung mit dem WirelessDevices massenweise zu trennen MulticastGroup	Schreiben	MulticastGroup*		
StartFuotaTask	Erteilt die Erlaubnis zum Starten von FuotaTask	Schreiben	FuotaTask*		
StartMulticastGroupSession	Erteilt die Erlaubnis zum Starten der MulticastGroup Sitzung	Schreiben	MulticastGroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartNetworkAnalyzerStream	Erteilt die Erlaubnis, den NetworkAnalyzer Stream zu starten	Schreiben	NetworkAnalyzerConfiguration*		
StartSingleWirelessDeviceImportTask	Gewährt die Berechtigung zum Starten der Importaufgabe für einzelne drahtlose Geräte	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
StartWirelessDeviceImportTask	Gewährt die Berechtigung zum Starten der Importaufgabe für drahtlose Geräte	Schreiben	ImportTask*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Gewährt die Berechtigung zum Markieren einer bestimmten Ressource mit Tags	Markieren	Destination		
			DeviceProfile		
			FuotaTask		
			ImportTask		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			MulticastGroup		
			NetworkAnalyzerConfiguration		
			ServiceProfile		
			SidewalkAccount		
			WirelessDevice		
			WirelessGateway		
			WirelessGatewayTaskDefinition		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TestWirelessDevice	Gewährt die Berechtigung zum Simulieren eines bereitgestellten Geräts, um Uplink-Daten mit der Nutzlast „Hello“ zu senden	Write	WirelessDevice*		
UntagResource	Gewährt die Berechtigung zum Entfernen der angegebenen Tags aus der Ressource	Markieren	Destination		
			DeviceProfile		
			FuotaTask		
			ImportTask		
			MulticastGroup		
			NetworkAnalyzerConfiguration		
			ServiceProfile		
			SidewalkAccount		
			WirelessDevice		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			WirelessGateway		
			WirelessGatewayTaskDefinition		
				aws:TagKeys	
UpdateDestination	Gewährt die Berechtigung zum Aktualisieren einer Zielressource	Schreiben	Destination*		
UpdateEventConfigurationByResourceTypes	Gewährt die Berechtigung zum Aktualisieren der Ereigniskonfiguration nach Ressourcentypen	Schreiben			
UpdateFuotaTask	Erteilt die Erlaubnis zur Aktualisierung des FuotaTask	Schreiben	FuotaTask*		
UpdateLogLevelsByResourceTypes	Gewährt Berechtigung zum Aktualisieren von Protokollebenen nach Ressourcentypen	Schreiben			
UpdateMetricConfiguration	Erteilt die Berechtigung zum Aktualisieren der Metrikkonfiguration	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateMulticastGroup	Erteilt die Erlaubnis zur Aktualisierung der Multicast Group	Schreiben	MulticastGroup*		
UpdateNetworkAnalyzerConfiguration	Erteilt die Erlaubnis zur Aktualisierung des NetworkAnalyzerConfiguration	Schreiben	MulticastGroup*		
			NetworkAnalyzerConfiguration*		
			WirelessDevice*		
			WirelessGateway*		
UpdatePartnerAccount	Gewährt die Berechtigung zum Aktualisieren eines Partnerkontos	Schreiben	SidewalkAccount*		
UpdatePosition	Gewährt die Berechtigung zum Aktualisieren von Positionen für eine Ressource	Schreiben	WirelessDevice		
			WirelessGateway		
UpdateResourceEventConfiguration	Gewährt die Berechtigung zum Aktualisieren einer Ereigniskonfiguration für eine Kennung	Schreiben	SidewalkAccount		
			WirelessDevice		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			WirelessGateway		
UpdateResourcePosition	Gewährt die Berechtigung zum Aktualisieren von Positionen für eine Ressource	Schreiben	WirelessDevice		
			WirelessGateway		
UpdateWirelessDevice	Erteilt die Berechtigung zum Aktualisieren einer WirelessDevice Ressource	Schreiben	WirelessDevice*		
UpdateWirelessDeviceImportTask	Gewährt die Berechtigung zum Aktualisieren einer Importaufgabe für drahtlose Geräte	Schreiben	ImportTask*		
UpdateWirelessGateway	Erteilt die Berechtigung zum Aktualisieren einer WirelessGateway Ressource	Schreiben	WirelessGateway*		

Von AWS IoT Wireless definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
WirelessDevice	arn:${Partition}:iotwireless:${Region}:${Account}:WirelessDevice/${WirelessDeviceId}	aws:ResourceTag/${TagKey}
WirelessGateway	arn:${Partition}:iotwireless:${Region}:${Account}:WirelessGateway/${WirelessGatewayId}	aws:ResourceTag/${TagKey}
DeviceProfile	arn:${Partition}:iotwireless:${Region}:${Account}:DeviceProfile/${DeviceProfileId}	aws:ResourceTag/${TagKey}
ServiceProfile	arn:${Partition}:iotwireless:${Region}:${Account}:ServiceProfile/${ServiceProfileId}	aws:ResourceTag/${TagKey}
Destination	arn:${Partition}:iotwireless:${Region}:${Account}:Destination/${DestinationName}	aws:ResourceTag/${TagKey}
SidewalkAccount	arn:${Partition}:iotwireless:${Region}:${Account}:SidewalkAccount/${SidewalkAccountId}	aws:ResourceTag/${TagKey}
WirelessGatewayTaskDefinition	arn:${Partition}:iotwireless:${Region}:${Account}:WirelessGatewayTaskDefinition/${WirelessGatewayTaskDefinitionId}	aws:ResourceTag/${TagKey}
FuotaTask	arn:${Partition}:iotwireless:${Region}:${Account}:FuotaTask/${FuotaTaskId}	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
Multicast Group	`arn:${Partition}:iotwireless:${Region}:${Account}:MulticastGroup/${MulticastGroupId}`	aws:ResourceTag/${TagKey}
NetworkAnalyzerConfiguration	`arn:${Partition}:iotwireless:${Region}:${Account}:NetworkAnalyzerConfiguration/${NetworkAnalyzerConfigurationName}`	aws:ResourceTag/${TagKey}
thing	`arn:${Partition}:iot:${Region}:${Account}:thing/${ThingName}`	
cert	`arn:${Partition}:iot:${Region}:${Account}:cert/${Certificate}`	
ImportTask	`arn:${Partition}:iotwireless:${Region}:${Account}:ImportTask/${ImportTaskId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS IoT Wireless

AWS IoT Wireless definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Zugriff nach einem Tag-Schlüssel, der in der Anforderung des Benutzers an IoT Wireless enthalten ist	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert Zugriff nach der Tag-Schlüsselkomponente eines Tags, das an eine IoT Wireless-Ressource angefügt ist	String
aws:TagKeys	Filtert Zugriff nach der Liste aller Tag-Schlüsselnamen, die der Ressource in der Anforderung zugeordnet sind	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS IQ

AWS IQ (Service-Präfix: `iq`) bietet die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Durch AWS IQ definierte Aktionen
- Durch AWS IQ definierte Ressourcentypen
- Bedingungsschlüssel für AWS IQ

Durch AWS IQ definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptCall	Gewährt die Berechtigung zum Annehmen eines eingehenden Sprach-/Videoanrufs	Schreiben	call*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ApprovePaymentRequest	Gewährt die Berechtigung zum Genehmigen einer Zahlungsanforderung	Schreiben	paymentRequest*		
ApproveProposal	Gewährt die Berechtigung zum Genehmigen eines Vorschlags	Schreiben	proposal*		
ArchiveConversation	Gewährt die Berechtigung zum Archivieren einer Konversation	Schreiben	conversation*		
CompleteProposal	Gewährt die Berechtigung zum Abschließen eines Vorschlags	Schreiben	proposal*		
CreateConversation	Gewährt die Berechtigung zum Antworten auf eine Anfrage oder zum Senden einer Direktnachricht, um eine Konversation zu beginnen	Schreiben			
CreateExpert	Gewährt die Berechtigung zum Erstellen eines Expertenprofils	Schreiben			
CreateListing	Gewährt die Berechtigung zum Erstellen eines Angebots	Schreiben			
CreateMilestoneProposal	Gewährt die Berechtigung zum Erstellen eines Meilensteinvorschlags	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreatePaymentRequest	Gewährt die Berechtigung zum Erstellen einer Zahlungsanforderung	Schreiben			
CreateProject	Gewährt die Berechtigung zum Senden neuer Anforderungen	Schreiben			
CreateRequest	Gewährt die Berechtigung zum Senden neuer Anforderungen	Schreiben			
CreateScheduledProposal	Gewährt die Berechtigung zum Erstellen eines geplanten Vorschlags	Schreiben			
CreateSeller	Gewährt die Berechtigung zum Erstellen eines Verkäuferprofils	Schreiben			
CreateUpfrontProposal	Gewährt die Berechtigung zum Erstellen eines Vorabvorschlags	Schreiben			
DeclineCall	Gewährt die Berechtigung zum Ablehnen eines eingehenden Sprach-/Videoanrufs	Schreiben	call*		
DeleteAttachment	Gewährt die Berechtigung zum Löschen eines vorhandenen Anhangs	Schreiben	attachment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisableIndividualPublicProfile	Gewährt die Berechtigung, eine individuelle öffentliche Profilseite zu deaktivieren	Schreiben	expert*		
DownloadAttachment	Gewährt die Berechtigung zum Herunterladen eines vorhandenen Anhangs	Lesen	attachment*		
EnableIndividualPublicProfile	Gewährt die Berechtigung, eine individuelle öffentliche Profilseite zu aktivieren	Schreiben	expert*		
EndCall	Gewährt die Berechtigung zum Beenden eines Sprach-/Videoanrufs	Schreiben	call*		
GetBuyer	Gewährt die Berechtigung zum Lesen von Käuferinformationen	Lesen	buyer*		
GetCall	Gewährt die Berechtigung zum Lesen von Informationen eines Sprach-/Videoanrufs	Lesen	call*		
GetChatInfo	Gewährt die Berechtigung zum Lesen der Chat-Umgebungsdetails einer Konversation	Lesen	conversation*		
GetChatMessages	Gewährt die Berechtigung zum Lesen von Chat-Nachrichten in einer Konversation	Lesen	conversation*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetChatToken	Gewährt die Berechtigung zur Anforderung eines Websocket-Token für die Konversationsbenachrichtigungen	Lesen	token*		
GetCompanyChatMessages	Gewährt die Berechtigung, Chat-Nachrichten in einer Unternehmenskonversation zu lesen	Lesen	conversation*		
GetCompanyProfile	Gewährt die Berechtigung zum Lesens eines Unternehmensprofils	Lesen	company*		
GetConversation	Gewährt die Berechtigung zum Lesen von Details einer Konversation	Lesen	conversation*		
GetExpert	Gewährt die Berechtigung zum Lesen von Experteninformationen	Lesen	expert*		
GetListing	Gewährt die Berechtigung zum Lesen eines Angebots	Lesen	listing*		
GetMarketplaceSeller	Gewährt die Berechtigung zum Lesen der Informationen eines Verkäuferprofils	Lesen	seller*		
GetPaymentRequest	Gewährt die Berechtigung zum Lesen einer Zahlungsanforderung	Lesen	paymentRequest*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetProposal	Gewährt die Berechtigung zum Lesen eines Vorschlags	Lesen	proposal*		
GetRequest	Gewährt die Berechtigung zum Abrufen einer erstellten Anforderung	Lesen	request*		
GetReview	Gewährt die Berechtigung zum Lesen einer Bewertung für einen Experten	Lesen	seller*		
HideRequest	Gewährt die Berechtigung zum Ausblenden einer Anfrage	Schreiben	request*		
InitiateCall	Gewährt die Berechtigung zum Starten eines Sprach-/Videoanrufs	Schreiben			
LinkAwsCertification	Gewährt die Berechtigung, eine AWS-Zertifizierung mit einem individuellen Profil zu verknüpfen	Schreiben	expert*		
ListAttachments	Gewährt die Berechtigung zum Auflisten bestehender Anhänge	Auflisten	attachment*		
ListConversations	Gewährt die Berechtigung zum Auflisten bestehender Konversationen	Lesen	conversation*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListExpertAccessLogs	Gewährt die Berechtigung, Zugriffsprotokolle von Expertenaktivitäten aufzulisten	Lesen	permission*		
ListListings	Gewährt die Berechtigung zum Auflisten von Angeboten	Lesen	listing*		
ListPaymentRequests	Gewährt die Berechtigung zum Auflisten einer Zahlungsanfrage	Lesen	paymentRequest		
			paymentSchedule		
ListProposals	Gewährt die Berechtigung zum Auflisten von Vorschlägen	Lesen	proposal*		
ListRequests	Gewährt die Berechtigung zum Auflisten von erstellten Anfragen	Lesen	request*		
ListReviews	Gewährt die Berechtigung zum Auflisten von Bewertungen für einen Experten	Lesen	seller*		
MarkChatMessageRead	Gewährt die Berechtigung zum Markieren einer Nachricht in einer Konversation als „gelesen“	Schreiben	conversation*		
RejectPaymentRequest	Gewährt die Berechtigung zum Ablehnen einer Zahlungsanforderung	Schreiben	paymentRequest*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RejectProposal	Gewährt die Berechtigung zum Ablehnen eines Vorschlags	Schreiben	proposal*		
SendCompanyChatMessage	Gewährt die Berechtigung zum Senden einer Nachricht in einer Konversation als Unternehmen	Schreiben	conversation*		
SendIndividualChatMessage	Gewährt die Berechtigung zum Senden einer Nachricht in einer Konversation als Einzelperson	Schreiben	conversation*		
UnarchiveConversation	Gewährt die Berechtigung zum Aufheben der Archivierung einer Konversation	Schreiben	conversation*		
UnlinkAwsCertification	Gewährt die Berechtigung, die Verknüpfung einer AWS-Zertifizierung mit einem individuellen Profil aufzuheben	Schreiben	expert*		
UpdateCompanyProfile	Gewährt die Berechtigung zum Aktualisieren eines Unternehmensprofils	Schreiben	company*		
UpdateConversationMembers	Gewährt die Berechtigung zum Hinzufügen weiterer Teilnehmer zu einer Konversation	Schreiben	conversation*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateExpert	Gewährt die Berechtigung zum Aktualisieren von Experteninformationen	Schreiben	expert*		
UpdateListing	Gewährt die Berechtigung zum Aktualisieren eines Angebots	Schreiben	listing*		
UpdateRequest	Gewährt die Berechtigung zum Aktualisieren einer Anfrage	Schreiben	request*		
UploadAttachment	Gewährt die Berechtigung zum Aktualisieren eines Anhangs	Schreiben			
WithdrawPaymentRequest	Gewährt die Berechtigung zum Zurückziehen einer Zahlungsanforderung	Schreiben	paymentRequest*		
WithdrawProposal	Gewährt die Berechtigung zum Zurückziehen eines Vorschlags	Schreiben	proposal*		
WriteReview	Gewährt die Berechtigung zum Schreiben einer Bewertung für einen Experten	Schreiben	seller*		

Durch AWS IQ definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden

können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
conversation	`arn:${Partition}:iq:${Region}::conversation/${ConversationId}`	
buyer	`arn:${Partition}:iq:${Region}::buyer/${BuyerId}`	
expert	`arn:${Partition}:iq:${Region}::expert/${ExpertId}`	
call	`arn:${Partition}:iq:${Region}::call/${CallId}`	
token	`arn:${Partition}:iq:${Region}::token/${TokenId}`	
proposal	`arn:${Partition}:iq:${Region}::proposal/${ConversationId}/${ProposalId}`	
paymentRequest	`arn:${Partition}:iq:${Region}::paymentRequest/${ConversationId}/${ProposalId}/${PaymentRequestId}`	
paymentSchedule	`arn:${Partition}:iq:${Region}::paymentSchedule/${ConversationId}/${ProposalId}/${VersionId}`	
seller	`arn:${Partition}:iq:${Region}::seller/${SellerAwsAccountId}`	
company	`arn:${Partition}:iq:${Region}::company/${CompanyId}`	

Ressource ntypen	ARN	Bedingungsschlüssel
request	`arn:${Partition}:iq:${Region}::request/${RequestId}`	
listing	`arn:${Partition}:iq:${Region}::listing/${ListingId}`	
attachment	`arn:${Partition}:iq:${Region}::attachment/${AttachmentId}`	
permission	`arn:${Partition}:iq-permission:${Region}::permission/${PermissionRequestId}`	

Bedingungsschlüssel für AWS IQ

IQ besitzt keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS IQ Berechtigungen

AWS IQ Berechtigungen (Service-Präfix: `iq-permission`) bietet die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Durch AWS IQ Berechtigungen definierte Aktionen
- Durch AWS IQ Berechtigung definierte Ressourcentypen
- Bedingungsschlüssel für AWS IQ-Berechtigungen

Durch AWS IQ Berechtigungen definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ApproveAccessGrant	Gewährt die Berechtigung zum Genehmigen einer Berechtigungsanfrage	Schreiben	permission*		
ApprovePermissionRequest	Gewährt die Berechtigung zum Genehmigen einer Berechtigungsanfrage	Schreiben	permission*		
AssumePermissionRole	Erteilt die Berechtigung, eine Reihe von temporären Sicherheitsnachweisen für Experten zu erhalten, mit denen diese auf die AWS-Ressourcen der Käufer zugreifen können	Schreiben	permission*		
CreatePermissionRequest	Gewährt die Berechtigung zum Erstellen einer Berechtigungsanfrage	Schreiben	permission*		
GetPermissionRequest	Gewährt die Berechtigung zum Abrufen einer Berechtigungsanfrage	Lesen	permission*		
ListPermissionRequests	Gewährt die Berechtigung zum Auflisten einer Berechtigungsanfrage	Lesen	permission*		
RejectPermissionRequest	Gewährt die Berechtigung zum Ablehnen einer Berechtigungsanfrage	Schreiben	permission*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RevokePermissionRequest	Gewährt die Berechtigung zum Widerrufen einer Berechtigung, die zuvor genehmigt wurde	Schreiben	permission*		
WithdrawPermissionRequest	Gewährt die Berechtigung, eine Genehmigungsanfrage zurückzuziehen, die nicht genehmigt oder abgelehnt wurde	Schreiben	permission*		

Durch AWS IQ Berechtigung definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
permission	`arn:${Partition}:iq-permission:${Region}::permission/${PermissionRequestId}`	

Bedingungsschlüssel für AWS IQ-Berechtigungen

IQ Permission umfasst keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Kendra

Amazon Kendra (Servicepräfix: `kendra`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Kendra definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung

mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateEntitiesToExperience	Gewährt die Berechtigung zum Speichern von Prinzipal zuordnung im Index	Schreiben	experience*		
			index*		
AssociatePersonasToEntities	Definiert die spezifischen Berechtigungen von Benutzern oder Gruppen in Ihrer AWS-SSO-Identitäts	Schreiben	experience*		
			index*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	quelle mit Zugriff auf Ihr Amazon Kendra-Erlebnis				
BatchDeleteDocument	Gewährt die Berechtigung für Batch-Löschvorgänge für das Dokument	Schreiben	index*		
BatchDeleteFeaturedResultsSet	Gewährt die Berechtigung zum Löschen einer vorgestellten Ergebnismenge	Schreiben	featured-results-set*		
			index*		
BatchGetDocumentStatus	Gewährt die Berechtigung für einen Batch-Get-Document-Status	Lesen	index*		
BatchPutDocument	Gewährt die Berechtigung für Batch-Put-Vorgänge für das Dokument	Schreiben	index*		
ClearQuerySuggestions	Gewährt die Berechtigung zum Löschen der bisher generierten Vorschläge für einen bestimmten Index	Schreiben	index*		
CreateAccessControlConfiguration	Gewährt die Berechtigung zum Erstellen einer Konfiguration der Zugriffssteuerung	Schreiben	index*		
CreateDataSource	Gewährt die Berechtigung zum Erstellen einer Datenquelle	Schreiben	index*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExperience	Erstellt ein Amazon Kendra-Erlebnis, z. B. eine Suchanwendung	Schreiben	index*		
CreateFaq	Gewährt die Berechtigung zum Erstellen von FAQ	Schreiben	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFeaturedResultsSet	Gewährt die Berechtigung zum Erstellen einer erweiterten Ergebnismenge	Schreiben	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateIndex	Gewährt die Berechtigung zum Erstellen einer Eingabe.	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateQuerySuggestionsBlockList	Gewährt die Berechtigung zum Erstellen einer QuerySuggestions BlockList	Schreiben	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateThesaurus	Gewährt die Berechtigung zum Erstellen eines Thesaurus	Schreiben	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessControlConfiguration	Gewährt die Berechtigung zum Löschen einer Konfiguration für die Zugriffssteuerung	Schreiben	access-control-configuration*		
			index*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteDataSource	Gewährt die Berechtigung zum Löschen einer Datenquelle	Schreiben	data-source*		
			index*		
DeleteExperience	Löscht Ihre Amazon Kendra-Erfahrung, z. B. eine Suchanwendung	Schreiben	experience*		
			index*		
DeleteFaq	Gewährt die Berechtigung zum Löschen von FAQ	Schreiben	faq*		
			index*		
DeleteIndex	Gewährt die Berechtigung zum Löschen eines Index	Schreiben	index*		
DeletePrincipalMapping	Gewährt die Berechtigung zum Löschen einer Prinzipal zuordnung vom Index	Schreiben	index*		
			data-source		
DeleteQuerySuggestionsBlockList	Gewährt die Berechtigung zum Löschen einer QuerySuggestions BlockList	Schreiben	index*		
			query-suggestions-block-list*		
DeleteThesaurus	Gewährt die Berechtigung zum Löschen eines Thesaurus	Schreiben	index*		
			thesaurus*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeAccessControlConfiguration	Gewährt die Berechtigung zum Beschreiben einer Konfiguration für die Zugriffssteuerung	Lesen	access-control-configuration*		
			index*		
DescribeDataSource	Gewährt die Berechtigung zum Beschreiben einer Datenquelle	Lesen	data-source*		
			index*		
DescribeExperience	Ruft Informationen über Ihre Amazon Kendra-Erfahrung, z. B. eine Suchanwendung, ab	Lesen	experience*		
			index*		
DescribeFaq	Gewährt die Berechtigung zum Beschreiben von FAQ	Lesen	faq*		
			index*		
DescribeFeaturedResultsSet	Gewährt die Berechtigung zum Beschreiben einer vorgestellten Ergebnismenge	Lesen	featured-results-set*		
			index*		
DescribeIndex	Gewährt die Berechtigung zum Beschreiben einer Eingabe.	Lesen	index*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribePrincipalMapping	Gewährt die Berechtigung zum Beschreiben von Prinzipalzuordnung aus dem Index	Lesen	index*		
			data-source		
DescribeQuerySuggestionsBlockList	Gewährt die Berechtigung zum Beschreiben einer QuerySuggestions BlockList	Lesen	index*		
			query-suggestions-block-list*		
DescribeQuerySuggestionsConfig	Gewährt die Berechtigung zum Beschreiben der Konfiguration der Abfragevorschläge für einen Index	Lesen	index*		
DescribeThesaurus	Gewährt die Berechtigung zum Beschreiben eines Thesaurus	Lesen	index*		
			thesaurus*		
DisassociateEntitiesFromExperience	Hindert Benutzer oder Gruppen in Ihrer AWS-SSO-Identitätsquelle am Zugriff auf Ihr Amazon Kendra-Erlebnis	Schreiben	experience*		
			index*		
DisassociatePersonasFromEntities	Entfernt die spezifischen Berechtigungen von Benutzern oder Gruppen in Ihrer AWS-SSO-Identitätsquelle mit Zugriff auf Ihr Amazon Kendra-Erlebnis	Schreiben	experience*		
			index*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetQuerySuggestions	Gewährt die Berechtigung zum Abrufen von Vorschlägen für ein Abfrage-Präfix	Lesen	index*		
GetSnapshots	Ruft Suchmetrikdaten ab	Lesen	index*		
ListAccessControlConfigurations	Gewährt die Berechtigung zum Auflisten der Konfigurationen für die Zugriffssteuerung	Auflisten	index*		
ListDataSourceSyncJobs	Gewährt die Berechtigung zum Abrufen des Verlaufs von Datenquellen-Synchronisierungsaufgaben	Auflisten	data-source*		
			index*		
ListDataSources	Gewährt die Berechtigung zum Auflisten der Datenquellen	Auflisten	index*		
ListEntityPersonas	Listet bestimmte Berechtigungen von Benutzern und Gruppen mit Zugriff auf Ihre Amazon Kendra-Erfahrung auf	Auflisten	experience*		
			index*		
ListExperienceEntities	Listet Benutzer oder Gruppen in Ihrer AWS-SSO-Identitätsquelle auf, denen Zugriff auf Ihre Amazon Kendra-Erfahrung gewährt wird	Auflisten	experience*		
			index*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListExperiences	Listet ein oder mehrere Amazon Kendra-Erlebnisse auf. Sie können ein Amazon Kendra-Erlebnis, z. B. eine Suchanwendung, erstellen	Auflisten	index*		
ListFaqs	Gewährt die Berechtigung zum Auflisten der FAQ	Auflisten	index*		
ListFeaturedResultsSets	Gewährt die Berechtigung zum Auflisten der vorgestellten Ergebnismengen	Auflisten	index*		
ListGroupsOlderThanOrderingId	Gewährt die Berechtigung zum Auflisten von Gruppen, die älter sind als eine Bestellnummer	Auflisten	index*		
			data-source		
ListIndices	Gewährt die Berechtigung zum Auflisten der Indizes	Auflisten			
ListQuerySuggestionsBlockLists	Gewährt die Berechtigung zum Auflisten von QuerySuggestions BlockLists	Auflisten	index*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen	data-source		
			faq		
			featured-results-set		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			index		
			query-suggestions-block-list		
			thesaurus		
ListThesauri	Gewährt die Berechtigung zum Auflisten der Thesauri	Auflisten	index*		
PutPrincipalMapping	Gewährt die Berechtigung zum Speichern von Prinzipal zuordnung im Index	Schreiben	index*		
			data-source		
Query	Gewährt die Berechtigung zum Abfragen von Dokumenten und FAQ	Lesen	index*		
Retrieve	Gewährt die Berechtigung, relevante Inhalte aus einem Index abzurufen	Lesen	index*		
StartDataSourceSyncJob	Gewährt die Berechtigung zum Starten einer Datenquellen-Synchronisierungsaufgabe	Schreiben	data-source*		
			index*		
StopDataSourceSyncJob	Gewährt die Berechtigung zum Anhalten einer Datenquellen-Synchronisierungsaufgabe	Schreiben	data-source*		
			index*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SubmitFeedback	Gewährt die Berechtigung zum Senden von Feedback zu Abfrageergebnissen	Schreiben	index*		
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit bestimmten Schlüsselwertpaaren	Markierung	data-source		
			faq		
			featured-results-set		
			index		
			query-suggestions-block-list		
			thesaurus		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung, das Tag mit dem angegebenen Schlüssel aus einer Ressource zu entfernen	Markierung	data-source		
			faq		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			featured-results-set		
			index		
			query-suggestions-block-list		
			thesaurus		
				aws:TagKeys	
UpdateAccessControlConfiguration	Gewährt die Berechtigung zum Aktualisieren einer Konfiguration für die Zugriffssteuerung	Schreiben	access-control-configuration*		
			index*		
UpdateDataSource	Gewährt die Berechtigung zum Aktualisieren einer Datenquelle	Schreiben	data-source*		
			index*		
UpdateExperience	Aktualisiert Ihr Amazon Kendra-Erlebnis, z. B. eine Suchanwendung	Schreiben	index*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateFeaturedResultsSet	Gewährt die Berechtigung zum Aktualisieren einer vorgestellten Ergebnismenge	Schreiben	featured-results-set*		
			index*		
UpdateIndex	Gewährt die Berechtigung zum Aktualisieren einer Eingabe.	Schreiben	index*		
UpdateQuerySuggestionsBlockList	Gewährt die Berechtigung zum Aktualisieren einer QuerySuggestions BlockList	Schreiben	index*		
			query-suggestions-block-list*		
UpdateQuerySuggestionsConfig	Gewährt die Berechtigung zum Aktualisieren der Konfiguration von Abfragevorschlägen für einen Index	Schreiben	index*		
UpdateThesaurus	Gewährt die Berechtigung zum Aktualisieren eines Thesaurus	Schreiben	index*		
			thesaurus*		

Von Amazon Kendra definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
index	`arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}`	aws:ResourceTag/${TagKey}
data-source	`arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/data-source/${DataSourceId}`	aws:ResourceTag/${TagKey}
faq	`arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/faq/${FaqId}`	aws:ResourceTag/${TagKey}
experience	`arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/experience/${ExperienceId}`	
thesaurus	`arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/thesaurus/${ThesaurusId}`	aws:ResourceTag/${TagKey}
query-suggestions-block-list	`arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/query-suggestions-block-list/${QuerySuggestionsBlockListId}`	aws:ResourceTag/${TagKey}
featured-results-set	`arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/featured-results-set/${FeaturedResultsSetId}`	aws:ResourceTag/${TagKey}
access-control-configuration	`arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/access-control-configuration/${AccessControlConfigurationId}`	

Bedingungsschlüssel für Amazon Kendra

Amazon Kendra definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Kendra Intelligent Ranking

Amazon Kendra Intelligent Ranking (Servicepräfix: `kendra-ranking`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Kendra Intelligent Ranking definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateRescoreExecutionPlan	Gewährt die Berechtigung zum Erstellen eines RescoreExecutionPlan	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteRescoreExecutionPlan	Gewährt die Berechtigung zum Löschen eines RescoreExecutionPlan	Schreiben	rescore-execution-plan*		
DescribeRescoreExecutionPlan	Gewährt die Berechtigung zum Beschreiben eines RescoreExecutionPlan	Lesen	rescore-execution-plan*		
ListRescoreExecutionPlans	Gewährt die Berechtigung zum Auflisten aller RescoreExecutionPlans	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen	rescore-execution-plan		
Rescore	Gewährt die Berechtigung zur erneuten Bewertung von Dokumenten mit Kendra Intelligent Ranking	Lesen	rescore-execution-plan*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit bestimmten Schlüsselwertpaaren	Markierung	rescore-execution-plan		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung, das Tag mit dem angegebenen Schlüssel aus einer Ressource zu entfernen	Markierung	rescore-execution-plan		
				aws:TagKeys	
UpdateRescoreExecutionPlan	Gewährt die Berechtigung zum Aktualisieren eines RescoreExecutionPlan	Schreiben	rescore-execution-plan*		

Von Amazon Kendra Intelligent Ranking definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
rescore-execution-plan	`arn:${Partition}:kendra-ranking:${Region}:${Account}:rescore-execution-plan/${RescoreExecutionPlanId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Kendra Intelligent Ranking

Amazon Kendra Intelligent Ranking definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Key Management Service

AWS Der Key Management Service (Dienstpräfix:`kms`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Key Management Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelKeyDeletion	Steuert die Berechtigung, das geplante Löschen eines KMS-Schlüssels abzubrechen AWS	Schreiben	key*		
				kms:CallerAccount kms:ViaService	
ConnectCustomKeyStore	Steuert die Berechtigung, einen benutzerdefinierten Schlüsselspeicher mit seinem zugehörigen AWS CloudHSM-Cluster oder externen Schlüsselmanager außerhalb von zu verbinden oder erneut zu verbinden AWS	Schreiben		kms:CallerAccount	
CreateAlias	Steuert die Berechtigung, einen Alias für einen AWS	Schreiben	alias*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	KMS-Schlüssel zu erstellen. Alias sind optionale Anzeigenamen, die Sie -KMS-Schlüsseln zuordnen können		key*		
				kms:CallerAccount kms:ViaService	
CreateCustomKeyStore	Steuert die Berechtigung zum Erstellen eines benutzerdefinierten Schlüsselspeichers, der von einem AWS CloudHSM-Cluster oder einem externen Schlüsselmanager außerhalb von AWS	Schreiben		kms:CallerAccount	cloudhsm:DescribeClusters iam:CreateServiceLinkedRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateGrant	Steuert die Berechtigung, einem AWS KMS-Schlüssel einen Grant hinzuzufügen. Sie können Berechtigungen verwenden, um Berechtigungen hinzuzufügen, ohne die Schlüsselrichtlinie oder IAM-Richtlinie zu ändern.	Berechtigungsverwaltung	key*	kms:CallerAccount kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:GrantConstraintType kms:GranteePrincipal kms:GrantIsForAWSResource kms:GrantOperations kms:RetiringPrincipal	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				kms:ViaService	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateKey	Steuert die Berechtigung zum Erstellen eines AWS KMS-Schlüssels, der zum Schutz von Datenschlüsseln und anderen vertraulichen Informationen verwendet werden kann	Schreiben		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys kms:BypassPolicyLockoutSafetyCheck kms:CallerAccount kms:KeySpec kms:KeyUsage kms:KeyOrigin kms:MultiRegion kms:MultiRegionKeyType	iam:CreateServiceLinkedRole kms:PutKeyPolicy kms:TagResource

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				kms:ViaService	
Decrypt	Steuert die Berechtigung zum Entschlüsseln von Chiffretext, der mit einem KMS-Schlüssel verschlüsselt wurde AWS	Schreiben	key*		
				kms:CallerAccount kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:RecipientAttestation:ImageSha384 kms:RequestAlias kms:ViaService	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteAlias	Steuert die Berechtigung zum Löschen eines Alias. Aliase sind optionale benutzerfreundliche Namen, die Sie KMS-Schlüsseln zuordnen können AWS	Schreiben	alias*		
			key*		
				kms:CallerAccount kms:ViaService	
DeleteCustomKeyStore	Steuert die Berechtigung zum Löschen eines benutzerdefinierten Schlüsselspeichers	Schreiben		kms:CallerAccount	
DeleteImportedKeyMaterial	Steuert die Berechtigung zum Löschen von kryptografischem Material, das Sie in einen AWS KMS-Schlüssel importiert haben. Diese Aktion macht den Schlüssel unbrauchbar.	Write	key*		
				kms:CallerAccount kms:ViaService	
DescribeCustomKeyStores	Steuert die Berechtigung zum Anzeigen detaillierter Informationen zu benutzerdefinierten Schlüsselspeichern im Konto und in der Region	Lesen		kms:CallerAccount	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeKey	Steuert die Berechtigung, detaillierte Informationen zu einem AWS KMS-Schlüssel einzusehen	Lesen	key*		
				kms:CallerAccount kms:RequestAlias kms:ViaService	
DisableKey	Steuert die Berechtigung zum Deaktivieren eines AWS KMS-Schlüssels, wodurch verhindert wird, dass er für kryptografische Operationen verwendet wird	Schreiben	key*		
				kms:CallerAccount kms:ViaService	
DisableKeyRotation	Steuert die Berechtigung, die automatische Rotation eines vom Kunden verwalteten AWS KMS-Schlüssels zu deaktivieren	Schreiben	key*		
				kms:CallerAccount kms:ViaService	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisconnectCustomKeyStore	Steuert die Berechtigung, den benutzerdefinierten Schlüsselspeicher von seinem zugehörigen AWS CloudHSM-Cluster oder externen Schlüsselmanager außerhalb von zu trennen AWS	Schreiben		kms:CallerAccount	
EnableKey	Steuert die Berechtigung, den Status eines AWS KMS-Schlüssels auf aktiviert zu ändern. Auf diese Weise kann der CMK in kryptografischen Produktionen verwendet werden.	Schreiben	key*		
				kms:CallerAccount kms:ViaService	
EnableKeyRotation	Steuert die Berechtigung, die automatische Rotation des kryptografischen Materials in einem AWS KMS-Schlüssel zu aktivieren	Schreiben	key*		
				kms:CallerAccount kms:RotationPeriodInDays kms:ViaService	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Encrypt	Steuert die Berechtigung, den angegebenen AWS KMS-Schlüssel zum Verschlüsseln von Daten und Datenschlüsseln zu verwenden	Schreiben	key*		
				kms:CallerAccount kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:RequestAlias kms:ViaService	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GenerateDataKey	Steuert die Erlaubnis, den AWS KMS-Schlüssel zum Generieren von Datenschlüsseln zu verwenden. Sie können die Datenschlüssel verwenden, um Daten außerhalb von AWS KMS zu verschlüsseln	Schreiben	key*		
				kms:CallerAccount kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:RecipientAttestation:ImageSha384 kms:RequestAlias kms:ViaService	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GenerateDataKeyPair	Steuert die Erlaubnis, den AWS KMS-Schlüssel zum Generieren von Datenschlüsselpaaren zu verwenden	Schreiben	key*		
				kms:CallerAccount kms:DataKeyPairSpec kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:RequestAlias kms:ViaService	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GenerateDataKeyPairWithoutPlaintext	Steuert die Erlaubnis, den AWS KMS-Schlüssel zum Generieren von Datenschlüsselpaaren zu verwenden. Im Gegensatz zur GenerateDataKeyPair Operation gibt diese Operation einen verschlüsselten privaten Schlüssel ohne Klartextkopie zurück	Schreiben	key*	kms:CallerAccount kms:DataKeyPairSpec kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:RequestAlias kms:ViaService	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GenerateDataKeyWithoutPlaintext	Steuert die Erlaubnis, den AWS KMS-Schlüssel zum Generieren eines Datenschlüssels zu verwenden. Im Gegensatz zur GenerateDataKey Operation gibt diese Operation einen verschlüsselten Datenschlüssel ohne Klartextversion des Datenschlüssels zurück	Schreiben	key*	kms:CallerAccount kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:RequestAlias kms:ViaService	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GenerateMac	Steuert die Erlaubnis, den AWS KMS-Schlüssel zur Generierung von Nachricht enauthentifizierungscodes zu verwenden	Schreiben	key*		
				kms:CallerAccount kms:MacAlgorithm kms:RequestAlias kms:ViaService	
GenerateRandom	Steuert die Erlaubnis, eine kryptografisch sichere zufällige Bytezeichenfolge von KMS abzurufen AWS	Schreiben		kms:RecipientAttestation:ImageSha384	
GetKeyPolicy	Steuert die Berechtigung, die Schlüsselrichtlinie für den angegebenen AWS KMS-Schlüssel einzusehen	Lesen	key*		
				kms:CallerAccount kms:ViaService	
GetKeyRotationStatus	Steuert die Berechtigung, den Schlüsselrotationsstatus für einen AWS KMS-Schlüssel einzusehen	Lesen	key*		
				kms:CallerAccount kms:ViaService	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetParametersForImport	Steuert die Berechtigung zum Abrufen von Daten, die zum Importieren von kryptografischem Material in einen vom Kunden verwalteten Schlüssel erforderlich sind, einschließlich eines öffentlichen Schlüssels und eines Import-Tokens	Lesen	key*		
				kms:CallerAccount kms:ViaService kms:WrappingAlgorithm kms:WrappingKeySpec	
GetPublicKey	Steuert die Berechtigung zum Herunterladen des öffentlichen Schlüssels eines asymmetrischen AWS KMS-Schlüssels	Lesen	key*		
				kms:CallerAccount kms:RequestAlias kms:ViaService	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ImportKeyMaterial	Steuert die Erlaubnis, kryptografisches Material in einen AWS KMS-Schlüssel zu importieren	Schreiben	key*		
				kms:CallerAccount kms:ExpirationModel kms:ValidTo kms:ViaService	
ListAliases	Steuert die Berechtigung zum Anzeigen der Alias, die im Konto definiert sind. Aliase sind optionale benutzerfreundliche Namen, die Sie KMS-Schlüsseln zuordnen AWS können	Auflisten			
ListGrants	Steuert die Berechtigung, alle Grants für einen AWS KMS-Schlüssel einzusehen	Auflisten	key*		
				kms:CallerAccount kms:GrantIsForAWSResource kms:ViaService	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListKeyPolicies	Steuert die Berechtigung, die Namen der wichtigsten Richtlinien für einen AWS KMS-Schlüssel anzuzeigen	Auflisten	key*		
				kms:CallerAccount kms:ViaService	
ListKeyRotations	Steuert die Berechtigung, die Liste der abgeschlossenen Schlüsselrotationen für einen AWS KMS-Schlüssel einzusehen	Auflisten	key*		
				kms:CallerAccount kms:ViaService	
ListKeys	Steuert die Berechtigung, die Schlüssel-ID und den Amazon-Ressourcennamen (ARN) aller AWS KMS-Schlüssel im Konto einzusehen	Auflisten			
ListResourceTags	Steuert die Berechtigung zum Anzeigen aller Tags, die an einen AWS KMS-Schlüssel angehängt sind	Auflisten	key*		
				kms:CallerAccount kms:ViaService	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListRetirableGrants	Steuert die Berechtigung zum Anzeigen der Erteilungen, in denen der angegebene Prinzipal der zurückziehende Prinzipal ist. Andere Prinzipale könnten in der Lage sein, die Berechtigung zurückzuziehen, und dieser Prinzipal könnte in der Lage sein, andere Berechtigungen zurückziehen.	Auflisten			
PutKeyPolicy	Steuert die Berechtigung, die Schlüsselrichtlinie für den angegebenen AWS KMS-Schlüssel zu ersetzen	Berechtigungsverwaltung	key*		
				kms:BypassPolicyLockoutSafetyCheck kms:CallerAccount kms:ViaService	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ReEncryptFrom	Steuert die Berechtigung zum Entschlüsseln von Daten als Teil des Prozesses, der die Daten innerhalb von KMS entschlüsselt und erneut verschlüsselt AWS	Schreiben	key*		
				kms:CallerAccount kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:ReEncryptOnSameKey kms:RequestAlias kms:ViaService	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ReEncryptTo	Steuert die Berechtigung zum Verschlüsseln von Daten als Teil des Prozesses, der die Daten innerhalb von KMS entschlüsselt und erneut verschlüsselt AWS	Schreiben	key*		
				kms:CallerAccount kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:ReEncryptOnSameKey kms:RequestAlias kms:ViaService	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ReplicateKey	Steuert die Berechtigung zum Replizieren eines Primärschlüssels mit mehreren Regionen	Write	key*		iam:CreateServiceLinkedRole kms:CreateKey kms:PutKeyPolicy kms:TagResource
				kms:CallerAccount kms:ReplicaRegion kms:ViaService	
RetireGrant	Steuert die Berechtigung zum Zurückziehen einer Berechtigung. Der RetireGrant Vorgang wird in der Regel vom Grant-Benutzer aufgerufen, nachdem er die Aufgaben abgeschlossen hat, zu deren Ausführung er im Rahmen der Grant-Lizenz berechtigt ist	Berechtigungsverwaltung	key*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RevokeGrant	Steuert die Berechtigung zum Widerrufen einer Berechtigung, wodurch alle Produktionen verweigert werden, die von der betreffenden Berechtigung abhängen	Berechtigungsverwaltung	key*		
				kms:CallerAccount kms:GrantIsForAWSResource kms:ViaService	
RotateKeyOnDemand	Steuert die Berechtigung, bei Bedarf die Rotation des kryptografischen Materials in einem AWS KMS-Schlüssel auszulösen	Schreiben	key*		
				kms:CallerAccount kms:ViaService	
ScheduleKeyDeletion	Steuert die Berechtigung, das Löschen eines KMS-Schlüssels zu planen AWS	Schreiben	key*		
				kms:CallerAccount kms:ScheduleKeyDeletionPendingWindowInDays kms:ViaService	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Sign	Steuert die Berechtigung zum Erstellen einer digitalen Signatur für eine Nachricht	Write	key*		
				kms:CallerAccount kms:MessageType kms:RequestAlias kms:SigningAlgorithm kms:ViaService	
SynchronizeMultiRegionKey [nur Berechtigung]	Steuert den Zugriff auf interne APIs, die Schlüssel für mehrere Regionen synchronisieren	Schreiben	key*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Steuert die Berechtigung zum Erstellen oder Aktualisieren von Tags, die an einen AWS KMS-Schlüssel angehängt sind	Tagging	key*		
				aws:RequestTag/${TagKey} aws:TagKeys kms:CallerAccount kms:ViaService	
UntagResource	Steuert die Berechtigung zum Löschen von Tags, die an einen AWS KMS-Schlüssel angehängt sind	Tagging	key*		
				aws:TagKeys kms:CallerAccount kms:ViaService	
UpdateAlias	Steuert die Berechtigung, einen Alias einem anderen AWS KMS-Schlüssel zuzuordnen. Ein Alias ist ein optionaler Anzeigename, den Sie einem Kundenmasterschlüssel zuordnen können.	Schreiben	alias*		
			key*		
				kms:CallerAccount kms:ViaService	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateCustomKeyStore	Steuert die Berechtigung zum Ändern der Eigenschaften eines benutzerdefinierten Schlüsselspeichers	Schreiben		kms:CallerAccount	
UpdateKeyDescription	Steuert die Berechtigung, die Beschreibung eines AWS KMS-Schlüssels zu löschen oder zu ändern	Schreiben	key*		
				kms:CallerAccount kms:ViaService	
UpdatePrimaryRegion	Steuert die Berechtigung zum Aktualisieren der primären Region eines Primärschlüssels mit mehreren Regionen	Schreiben	key*		
				kms:CallerAccount kms:PrimaryRegion kms:ViaService	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Verify	Steuert die Berechtigung, den angegebenen AWS KMS-Schlüssel zur Überprüfung digitaler Signaturen zu verwenden	Schreiben	key*		
				kms:CallerAccount kms:MessageType kms:RequestAlias kms:SigningAlgorithm kms:ViaService	
VerifyMac	Steuert die Erlaubnis, den AWS KMS-Schlüssel zur Überprüfung von Nachricht enauthentifizierungscodes zu verwenden	Schreiben	key*		
				kms:CallerAccount kms:MacAlgorithm kms:RequestAlias kms:ViaService	

Vom AWS Key Management Service definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
alias	`arn:${Partition}:kms:${Region}:${Account}:alias/${Alias}`	
key	`arn:${Partition}:kms:${Region}:${Account}:key/${KeyId}`	aws:ResourceTag/${TagKey} kms:KeyOrigin kms:KeySpec kms:KeyUsage kms:MultiRegion kms:MultiRegionKeyType kms:ResourceAliases

Bedingungsschlüssel für AWS Key Management Service

AWS Der Key Management Service definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff auf die angegebenen AWS KMS-Operationen auf der Grundlage des Schlüssels und des Werts des Tags in der Anfrage	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff auf die angegebenen AWS KMS-Operationen auf der Grundlage von Tags, die dem AWS KMS-Schlüssel zugewiesen sind	String
aws:TagKeys	Filtert den Zugriff auf die angegebenen AWS KMS-Operationen auf der Grundlage der Tagschlüssel in der Anfrage	ArrayOfString
kms:BypassPolicyLockoutSafetyCheck	Filtert den Zugriff auf die PutKeyPolicy Operationen CreateKey und basierend auf dem Wert des BypassPolicyLockoutSafetyCheck Parameters in der Anforderung	Bool
kms:CallerAccount	Filtert den Zugriff auf bestimmte AWS KMS-Operationen basierend auf der AWS-Konto ID des Anrufers. Sie können diesen Bedingungsschlüssel verwenden, um allen IAM-Benutzern und -Rollen AWS-Konto in einer einzigen Richtlinienanweisung den Zugriff zu gewähren oder zu verweigern	String
kms:CustomerMasterKeySpec	Der CustomerMasterKeySpec Bedingungsschlüssel kms: ist veraltet. Verwenden Sie stattdessen den Bedingungsschlüssel kms: KeySpec	String
kms:CustomerMasterKeyUsage	Der CustomerMasterKeyUsage Bedingungsschlüssel kms: ist veraltet. Verwenden Sie stattdessen den Bedingungsschlüssel kms: KeyUsage	String
kms:DataKeyPairSpec	Filtert den Zugriff auf GenerateDataKeyPair und die GenerateDataKeyPairWithoutPlaintext Operationen	String

Bedingungsschlüssel	Beschreibung	Typ
	basierend auf dem Wert des KeyPairSpec Parameters in der Anfrage	
kms:EncryptionAlgorithm	Filtert den Zugriff auf VerschlüsselungsProduktionen basierend auf dem Wert des Verschlüsselungsalgorithmus in der Anforderung	String
kms:EncryptionContext:${EncryptionContextKey}	Filtert den Zugriff auf einen symmetrischen AWS KMS-Schlüssel auf der Grundlage des Verschlüsselungskontextes in einem kryptografischen Vorgang. Diese Bedingung bewertet sowohl den Schlüssel als auch den Wert in jedem Verschlüsselungskontext-Paar	String
kms:EncryptionContextKeys	Filtert den Zugriff auf einen symmetrischen AWS KMS-Schlüssel auf der Grundlage des Verschlüsselungskontextes in einem kryptografischen Vorgang. Dieser Bedingungsschlüssel bewertet nur den Schlüssel in jedem Verschlüsselungskontext-Paar	ArrayOfString
kms:ExpirationModel	Filtert den Zugriff auf den ImportKeyMaterial Vorgang basierend auf dem Wert des ExpirationModel Parameters in der Anforderung	String
kms:GrantConstraintType	Filtert den Zugriff auf den CreateGrant Vorgang auf der Grundlage der Gewährungsbeschränkung in der Anfrage	String
kms:GrantIsForAWSResource	Filtert den Zugriff auf den CreateGrant Vorgang, wenn die Anfrage von einem bestimmten AWS Dienst stammt	Bool
kms:GrantOperations	Filtert den Zugriff auf die CreateGrant Operation basierend auf den Vorgängen im Zuschuss	ArrayOfString
kms:GranteePrincipal	Filtert den Zugriff auf den CreateGrant Vorgang auf der Grundlage des Prinzipals des Empfängers im Zuschuss	String

Bedingungsschlüssel	Beschreibung	Typ
kms:KeyOrigin	Filtert den Zugriff auf eine API-Operation auf der Grundlage der Origin-Eigenschaft des AWS KMS-Schlüssels, der durch den Vorgang erstellt oder in dem Vorgang verwendet wurde. Verwenden Sie diese Option, um die Autorisierung des CreateKey Vorgangs oder eines beliebigen Vorgangs, der für einen KMS-Schlüssel autorisiert ist, zu qualifizieren	String
kms:KeySpec	Filtert den Zugriff auf einen API-Vorgang auf der Grundlage der KeySpec Eigenschaft des AWS KMS-Schlüssels, der durch den Vorgang erstellt oder in dem Vorgang verwendet wurde. Verwenden Sie es, um die Autorisierung des CreateKey Vorgangs oder eines beliebigen Vorgangs, der für eine KMS-Schlüsselressource autorisiert ist, zu qualifizieren	String
kms:KeyUsage	Filtert den Zugriff auf eine API-Operation auf der Grundlage der KeyUsage Eigenschaft des AWS KMS-Schlüssels, der durch den Vorgang erstellt oder in dem Vorgang verwendet wurde. Verwenden Sie es, um die Autorisierung des CreateKey Vorgangs oder eines beliebigen Vorgangs, der für eine KMS-Schlüsselressource autorisiert ist, zu qualifizieren	String
kms:MacAlgorithm	Filtert den Zugriff auf die VerifyMac Operationen GenerateMac und auf der Grundlage des MacAlgorithm Parameters in der Anforderung	String
kms:MessageType	Filtert den Zugriff auf die Operationen „Signieren“ und „Überprüfen“ auf der Grundlage des MessageType Parameterwerts in der Anforderung	String

Bedingungsschlüssel	Beschreibung	Typ
kms:MultiRegion	Filtert den Zugriff auf eine API-Operation auf der Grundlage der MultiRegion Eigenschaft des AWS KMS-Schlüssels, der durch den Vorgang erstellt oder in dem Vorgang verwendet wurde. Verwenden Sie es, um die Autorisierung des CreateKey Vorgangs oder eines beliebigen Vorgangs, der für eine KMS-Schlüsselressource autorisiert ist, zu qualifizieren	Bool
kms:MultiRegionKeyType	Filtert den Zugriff auf eine API-Operation auf der Grundlage der MultiRegionKeyType Eigenschaft des AWS KMS-Schlüssels, der durch den Vorgang erstellt oder in dem Vorgang verwendet wurde. Verwenden Sie es, um die Autorisierung des CreateKey Vorgangs oder eines beliebigen Vorgangs, der für eine KMS-Schlüsselressource autorisiert ist, zu qualifizieren	String
kms:PrimaryRegion	Filtert den Zugriff auf den UpdatePrimaryRegion Vorgang basierend auf dem Wert des PrimaryRegion Parameters in der Anforderung	String
kms:ReEncryptOnSameKey	Filtert den Zugriff auf den ReEncrypt Vorgang, wenn er denselben AWS KMS-Schlüssel verwendet, der für den Verschlüsselungsvorgang verwendet wurde	Bool
kms:RecipientAttestation:ImageSha384	Filtert den Zugriff auf die GenerateRandom Operationen Decrypt und GenerateDataKey, die auf dem Bild-Hash im Bestätigungsdokument in der Anforderung basieren	String
kms:RecipientAttestation:PCR	Filtert den Zugriff auf Decrypt- GenerateDataKey und GenerateRandom -Operationen auf der Grundlage der Plattformkonfigurationsregister (PCRs) im Bescheinigungsdokument in der Anfrage	String

Bedingungsschlüssel	Beschreibung	Typ
kms:ReplicaRegion	Filtert den Zugriff auf den ReplicateKey Vorgang basierend auf dem Wert des Parameters in der Anforderung ReplicaRegion	String
kms:RequestAlias	Filtert den Zugriff auf kryptografische Operationen und GetPublicKey basiert auf dem Alias in der Anfrage DescribeKey	String
kms:ResourceAliases	Filtert den Zugriff auf bestimmte AWS KMS-Operationen auf der Grundlage von Aliasnamen, die AWS dem KMS-Schlüssel zugeordnet sind	ArrayOfString
kms:RetiringPrincipal	Filtert den Zugriff auf den CreateGrant Vorgang auf der Grundlage des ausscheidenden Schulleiters im Zuschuss	String
kms:RotationPeriodInDays	Filtert den Zugriff auf den EnableKeyRotation Vorgang basierend auf dem Wert des RotationPeriodInDays Parameters in der Anforderung	Numerischer Wert
kms:ScheduleKeyDeletionPendingWindowInDays	Filtert den Zugriff auf den ScheduleKeyDeletion Vorgang basierend auf dem Wert des PendingWindowInDays Parameters in der Anforderung	Numerischer Wert
kms:SigningAlgorithm	Filtert den Zugriff auf die Sign- und Verify-Produktionen basierend auf dem Signaturalgorithmus in der Anforderung	String
kms:ValidTo	Filtert den Zugriff auf den ImportKeyMaterial Vorgang basierend auf dem Wert des ValidTo Parameters in der Anforderung. Sie können diesen Bedingungsschlüssel verwenden, um Benutzern das Importieren von Schlüsselmaterial nur dann zu erlauben, wenn es zum angegebenen Datum abläuft.	Datum

Bedingungsschlüssel	Beschreibung	Typ
kms:ViaService	Filtert den Zugriff, wenn eine im Namen des Prinzipals gestellte Anfrage von einem bestimmten AWS Dienst stammt	String
kms:WrappingAlgorithm	Filtert den Zugriff auf den GetParametersForImport Vorgang basierend auf dem Wert des WrappingAlgorithm Parameters in der Anfrage	String
kms:WrappingKeySpec	Filtert den Zugriff auf den GetParametersForImport Vorgang basierend auf dem Wert des WrappingKeySpec Parameters in der Anforderung	String

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Keyspaces (für Apache Cassandra)

Amazon Keyspaces (für Apache Cassandra) (Service-Präfix: `cassandra`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien zur Verfügung.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Keyspaces definierte Aktionen (für Apache Cassandra) definierte Aktionen
- Von Amazon Keyspaces definierte Ressourcentypen (für Apache Cassandra)
- Bedingungsschlüssel für Amazon Keyspaces (für Apache Cassandra)

Von Amazon Keyspaces definierte Aktionen (für Apache Cassandra) definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Alter	Gewährt die Berechtigung zum Ändern eines Schlüsselraums oder einer Tabelle	Schreiben	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
AlterMultiRegionResource	Gewährt die Berechtigung zum Ändern eines Multiregion-Schlüsselraums oder einer -Tabelle	Schreiben	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
Create	Gewährt die Berechtigung zum Anlegen eines Schlüsselraums oder einer Tabelle	Schreiben	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
	Gewährt die Berechtigung zum Erstellem eines Multiregi	Schreiben	keyspace		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateMultiRegionResource	on-Schlüsselraums oder einer -Tabelle		table		
				aws:RequestTag/${TagKey} aws:TagKeys	
Drop	Gewährt die Berechtigung, einen Schlüsselraum oder eine Tabelle zu löschen	Schreiben	keyspace		
			table		
DropMultiRegionResource	Gewährt die Berechtigung zum Entfernen eines Multiregion-Schlüsselraums oder einer -Tabelle	Schreiben	keyspace		
			table		
Modify	Gewährt die Berechtigung zum INSERT, UPDATE oder DELETE von Daten in einer Tabelle	Schreiben	table*		
ModifyMultiRegionResource	Gewährt die Berechtigung zum Ausführen der Datenbefehle INSERT, UPDATE oder DELETE in einer Tabelle	Schreiben	table*		
Restore	Gewährt die Berechtigung zum Wiederherstellen einer Tabelle aus einem Backup	Schreiben	table*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
RestoreMultiRegionTable	Gewährt die Berechtigung zum Wiederherstellen einer Multiregion-Tabelle aus einem Backup	Schreiben	table*		
				aws:RequestTag/${TagKey} aws:TagKeys	
Select	Gewährt die Berechtigung zum SELECT von Daten aus einer Tabelle	Lesen	table*		
SelectMultiRegionResource	Gewährt die Berechtigung zum SELECT von Daten aus einer Multiregion-Tabelle	Lesen	table*		
TagMultiRegionResource	Gewährt die Berechtigung zum Markieren eines Multiregion-Schlüsselraums oder einer -Tabelle	Markierung	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Taggen eines Schlüsselraums oder einer Tabelle	Markierung	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
UnTagMultiRegionResource	Gewährt die Berechtigung zum Entfernen der Markierung eines Multiregion-Schlüsselraums oder einer -Tabelle	Markierung	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Tags für einen Schlüsselraum oder eine Tabelle	Markierung	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdatePartitioner	Gewährt die Berechtigung zum AKTUALISIEREN des Partitioners in einer Systemtabelle	Schreiben	table*		

Von Amazon Keyspaces definierte Ressourcentypen (für Apache Cassandra)

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
keyspace	`arn:${Partition}:cassandra:${Region}:${Account}:/keyspace/${KeyspaceName}/`	aws:ResourceTag/${TagKey}
table	`arn:${Partition}:cassandra:${Region}:${Account}:/keyspace/${KeyspaceName}/table/${TableName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Keyspaces (für Apache Cassandra)

Amazon Keyspaces (für Apache Cassandra) definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung.	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf den Tag-Schlüssel-Wert-Paaren, die an die Ressource angefügt wurden.	Zeichenfolge
aws:TagKeys	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Kinesis Analytics

Amazon Kinesis Analytics (Servicepräfix: `kinesisanalytics`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Kinesis Analytics definierte Aktionen
- Von Amazon Kinesis Analytics definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Kinesis Analytics

Von Amazon Kinesis Analytics definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddApplicationInput	Gewährt die Berechtigung, der Anwendung Eingaben hinzuzufügen	Schreiben	application*		
AddApplicationOutput	Gewährt die Berechtigung, der Anwendung eine Ausgabe hinzuzufügen	Write	application*		
AddApplicationReferenceDataSource	Gewährt die Berechtigung, der Anwendung eine Referenzdatenquelle hinzuzufügen	Schreiben	application*		
CreateApplication	Gewährt die Berechtigung zum Erstellen einer Anwendung	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Gewährt die Berechtigung zum Löschen einer Anwendung	Schreiben	application*		
DeleteApplicationOutput	Gewährt die Berechtigung zum Löschen der angegebenen Ausgabe der Anwendung	Write	application*		
DeleteApplicationReferenceDataSource	Gewährt die Berechtigung zum Löschen der angegebenen Referenzdatenquelle der Anwendung	Schreiben	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeApplication	Gewährt die Berechtigung, die angegebene Anwendung zu beschreiben	Lesen	application*		
DiscoverInputSchema	Gewährt die Berechtigung zum Erkennen des Eingabeschemas für die Anwendung	Lesen			
GetApplicationState [nur Berechtigung]	Gewährt die Berechtigung an die Kinesis Data Analytics-Konsole, Stream-Ergebnisse für Kinesis Data Analytics SQL-Laufzeitanwendungen anzuzeigen	Lesen	application*		
ListApplications	Gewährt die Berechtigung zum Auflisten von Anträgen für das Konto	List			
ListTagsForResource	Gewährt die Berechtigung, die mit Ihrer Ressource verknüpften Tags abzurufen	Read	application*		
StartApplication	Gewährt die Berechtigung zum Starten der Anwendung	Write	application*		
StopApplication	Gewährt die Erlaubnis, die Anwendung zu beenden	Write	application*		
TagResource	Gewährt die Berechtigung, der Anwendung Tags hinzuzufügen	Markieren	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen der angegebenen Tags aus der Applikation.	Markieren	application*		
				aws:TagKeys	
UpdateApplication	Gewährt die Berechtigung zum Aktualisieren einer Anwendung	Schreiben	application*		

Von Amazon Kinesis Analytics definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
application	`arn:${Partition}:kinesisanalytics:${Region}:${Account}:application/${ApplicationName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Kinesis Analytics

Amazon Kinesis Analytics definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den Werten für jedes der Tags	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Tag-Wert, der der Ressource zugeordnet ist	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach dem Vorhandensein verbindlicher Tag-Schlüssel in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Kinesis Analytics V2

Amazon Kinesis Analytics V2 (Servicepräfix: `kinesisanalytics`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Kinesis Analytics V2 definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddApplicationCloudWatchLoggingOption	Gewährt die Berechtigung zum Hinzufügen der Cloudwatch-Protokollierungsoption zur Anwendung	Write	application*		
AddApplicationInput	Gewährt die Berechtigung, der Anwendung Eingaben hinzuzufügen	Write	application*		
AddApplicationInputProcessingConfiguration	Gewährt die Berechtigung, der Anwendung eine Konfiguration für die Eingabeverarbeitung hinzuzufügen	Write	application*		
AddApplicationOutput	Gewährt die Berechtigung, der Anwendung eine Ausgabe hinzuzufügen	Write	application*		
AddApplicationReferenceDataSource	Gewährt die Berechtigung, der Anwendung eine Referenzdatenquelle hinzuzufügen	Write	application*		
AddApplicationVpcConfiguration	Gewährt die Berechtigung, der Anwendung eine VPC-Konfiguration hinzuzufügen	Write	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateApplication	Gewährt die Berechtigung zum Erstellen einer Anwendung	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
CreateApplicationPresignedUrl	Gewährt die Berechtigung zum Erstellen und Zurückgeben einer URL, mit der Sie eine Verbindung mit der Erweiterung einer Anwendung herstellen können	Read	application*		
CreateApplicationSnapshot	Gewährt die Berechtigung zum Erstellen eines Snapshots für eine Anwendung	Write	application*		
DeleteApplication	Gewährt die Berechtigung zum Löschen einer Anwendung	Write	application*		
DeleteApplicationCloudWatchLoggingOption	Gewährt die Berechtigung zum Löschen der angegebenen Cloudwatch-Protokollierungsoption der Anwendung	Write	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteApplicationInputProcessingConfiguration	Gewährt die Berechtigung zum Löschen der angegebenen Eingabeverarbeitungskonfiguration der Anwendung	Write	application*		
DeleteApplicationOutput	Gewährt die Berechtigung zum Löschen der angegebenen Ausgabe der Anwendung	Write	application*		
DeleteApplicationReferenceDataSource	Gewährt die Berechtigung zum Löschen der angegebenen Referenzdatenquelle der Anwendung	Write	application*		
DeleteApplicationSnapshot	Gewährt die Berechtigung zum Löschen eines Snapshots für eine Anwendung	Write	application*		
DeleteApplicationVpcConfiguration	Gewährt die Berechtigung zum Löschen der angegebenen VPC-Konfiguration der Anwendung	Write	application*		
DescribeApplication	Gewährt die Berechtigung, die angegebene Anwendung zu beschreiben	Read	application*		
DescribeApplicationSnapshot	Gewährt die Berechtigung zur Beschreibung eines Anwendungssnapshot	Lesen	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeApplicationVersion	Gewährt die Berechtigung zum Löschen einer Anwendungsversion aus einer Anwendung.	Lesen	application*		
DiscoverInputSchema	Gewährt die Berechtigung zum Erkennen des Eingabeschemas für die Anwendung	Read			iam:PassRole
ListApplicationSnapshots	Gewährt die Berechtigung zum Auflisten der Snapshots für eine Anwendung	Lesen	application*		
ListApplicationVersions	Gewährt die Berechtigung zum Löschen einer Anwendungsversion aus einer Anwendung.	Lesen	application*		
ListApplications	Gewährt die Berechtigung zum Auflisten von Anträgen für das Konto	List			
ListTagsForResource	Gewährt die Berechtigung, die mit Ihrer Ressource verknüpften Tags abzurufen	Lesen	application*		
RollbackApplication	Gewährt die Berechtigung zum Ausführen eines Rollback-Vorgangs für eine Anwendung	Schreiben	application*		
StartApplication	Gewährt die Berechtigung zum Starten der Anwendung	Write	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopApplication	Gewährt die Erlaubnis, die Anwendung zu beenden	Write	application*		
TagResource	Gewährt die Berechtigung, der Anwendung Tags hinzuzufügen	Markieren	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen der angegebenen Tags aus der Applikation.	Markieren	application*		
				aws:TagKeys	
UpdateApplication	Gewährt die Berechtigung zum Aktualisieren einer Anwendung	Schreiben	application*		
UpdateApplicationMaintenanceConfiguration	Gewährt die Berechtigung zum Aktualisieren der Wartungskonfiguration einer Anwendung	Schreiben	application*		

Von Amazon Kinesis Analytics V2 definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der

Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
application	`arn:${Partition}:kinesisanalytics:${Region}:${Account}:application/${ApplicationName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Kinesis Analytics V2

Amazon Kinesis Analytics V2 definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den Werten für jedes der Tags	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Tag-Wert, der der Ressource zugeordnet ist	String
aws:TagKeys	Filtert den Zugriff nach dem Vorhandensein verbindlicher Tag-Schlüssel in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Kinesis Data Streams

Amazon Kinesis Data Streams (Servicepräfix: `kinesis`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungsschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Kinesis Data Streams definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddTagsToStream	Erteilt die Berechtigung zum Hinzufügen oder Aktualisieren von Tags für den angegebenen Amazon Kinesis-Stream Jeder Stream kann bis zu 10 Tags aufweisen.	Markierung	stream*		
CreateStream	Erteilt die Berechtigung, einen Amazon Kinesis-Stream zu erstellen	Schreiben	stream*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DecreaseStreamRetentionPeriod	Erteilt die Berechtigung, den Aufbewahrungszeitraum des Streams zu verringern. Dabei handelt es sich um den Zeitraum, in dem auf Datensätze zugegriffen werden kann, nachdem sie dem Stream hinzugefügt wurden	Schreiben	stream*		
DeleteResourcePolicy	Gewährt die Berechtigung zum Löschen einer Ressourcenrichtlinie, die dem angegebenen Stream oder Verbraucher zugeordnet ist	Schreiben	consumer* stream*		
DeleteStream	Erteilt die Berechtigung zum Löschen eines Streams all seiner Shards und Daten	Schreiben	stream*		
DeregisterStreamConsumer	Erteilt die Berechtigung, die Registrierung eines Stream-Konsumenten bei einem Kinesis-Datenstrom aufzuheben	Schreiben	consumer*		
DescribeLimits	Erteilt die Berechtigung zum Beschreiben der Shard-Limits für das Benutzerkonto	Lesen			
DescribeStream	Erteilt die Berechtigung zum Beschreiben des angegebenen Streams	Lesen	stream*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeStreamConsumer	Erteilt die Berechtigung, die Beschreibung eines registrierten Stream-Konsumenten abzurufen	Lesen	consumer*		
DescribeStreamSummary	Erteilt die Berechtigung, eine zusammenfassende Beschreibung des angegebenen Kinesis-Datenstroms ohne die Shard-Liste bereitzustellen	Lesen	stream*		
DisableEnhancedMonitoring	Erteilt die Berechtigung zum Deaktivieren der erweiterten Überwachung	Schreiben			
EnableEnhancedMonitoring	Erteilt die Berechtigung zur Aktivierung einer erweiterten Kinesis-Datenstrom-Überwachung für Shard-Level-Metriken	Schreiben			
GetRecords	Erteilt die Berechtigung zum Abrufen von Datensätzen von einem Shard	Lesen	stream*		
GetResourcePolicy	Gewährt die Berechtigung zum Abrufen einer Ressourcenrichtlinie, die dem angegebenen Stream oder Verbraucher zugeordnet ist	Lesen	consumer* stream*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetShardIterator	Erteilt die Berechtigung einen Shard-Iterator abzurufen Ein Shard-Iterator läuft fünf Minuten nach Rückgabe an den Auftraggeber ab	Lesen	stream*		
IncreaseStreamRetentionPeriod	Erteilt die Berechtigung, den Aufbewahrungszeitraum des Streams, also den Zeitraum, in dem auf Datensätze zugegriffen werden kann, nachdem sie dem Stream hinzugefügt wurden, zu erhöhen	Schreiben	stream*		
ListShards	Erteilt die Berechtigung, die Shards in einem Stream aufzulisten und Informationen zu jedem Shard bereitzustellen	Auflisten	stream*		
ListStreamConsumers	Erteilt die Berechtigung, die Stream-Konsumenten aufzulisten, die für den Empfang von Daten von einem Kinesis-Stream mit erweiterten Rundsendungen registriert sind und Informationen über die einzelnen Konsumenten bereitzustellen	Auflisten	stream*		
ListStreams	Erteilt die Berechtigung zum Auflisten Ihrer Streams	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForStream	Erteilt die Berechtigung zum Auflisten der Tags für den angegebenen Amazon Kinesis-Stream	Lesen	stream*		
MergeShards	Erteilt die Berechtigung, zwei benachbarte Shards in einem einzelnen Stream zusammenzuführen, um die Kapazität des Streams zum Annehmen und Übertragen von Daten zu reduzieren	Schreiben	stream*		
PutRecord	Erteilt die Berechtigung, einen einzelnen Datensatz aus einem Produzenten in einen Amazon Kinesis-Stream zu schreiben	Schreiben	stream*		
PutRecords	Erteilt die Berechtigung, in einem Aufruf mehrere Datensätze aus einem Produzenten in einen Amazon Kinesis-Stream zu schreiben (wird auch als PutRecords-Anforderung bezeichnet)	Schreiben	stream*		
PutResourcePolicy	Gewährt die Berechtigung zum Anfügen einer Ressourcenrichtlinie an einen angegebenen Stream oder Verbraucher.	Schreiben	consumer* stream*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RegisterStreamConsumer	Erteilt die Berechtigung, einen Stream-Konsumenten bei einem Kinesis-Datenstrom zu registrieren	Schreiben	stream*		
RemoveTagsFromStream	Erteilt die Berechtigung zum Entfernen von Tags aus dem angegebenen Kinesis-Datenstrom Entfernte Tags werden gelöscht und können nicht wiederhergestellt werden, nachdem dieser Vorgang erfolgreich abgeschlossen wurde	Markierung	stream*		
SplitShard	Erteilt die Berechtigung, einen Shard in zwei neue Shards im Kinesis-Datenstrom aufzuteilen, um die Kapazität des Streams zum Annehmen und Übertragen von Daten zu erhöhen	Schreiben	stream*		
StartStreamEncryption	Erteilt die Berechtigung zum Aktivieren oder Aktualisieren der serverseitigen Verschlüsselung unter Verwendung eines AWS-KMS-Schlüssels für einen angegebenen Stream.	Schreiben	kmsKey* stream*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopStreamEncryption	Erteilt die Berechtigung, die serverseitige Verschlüsselung für einen angegebenen Stream zu deaktivieren	Schreiben	kmsKey*		
			stream*		
SubscribeToShard	Erteilt die Berechtigung zur Überwachung eines bestimmten Shards mit erweitertem fan-out	Lesen	consumer*		
UpdateShardCount	Erteilt die Berechtigung, die Shard-Anzahl des angegebenen Streams auf die angegebene Anzahl von Shards zu aktualisieren	Schreiben			
UpdateStreamMode	Erteilt die Berechtigung zum Aktualisieren des Kapazitätsmodus des Datenstroms	Schreiben			

Von Amazon Kinesis Data Streams definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
stream	`arn:${Partition}:kinesis:${Region}:${Account}:stream/${StreamName}`	
consumer	`arn:${Partition}:kinesis:${Region}:${Account}:${StreamType}/${StreamName}/consumer/${ConsumerName}:${ConsumerCreationTimpstamp}`	
kmsKey	`arn:${Partition}:kms:${Region}:${Account}:key/${KeyId}`	

Bedingungsschlüssel für Amazon Kinesis Data Streams

Kinesis besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Kinesis Firehose

Amazon Kinesis Firehose (Servicepräfix: `firehose`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Kinesis Firehose definierte Aktionen

- Von Amazon Kinesis Firehose definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Kinesis Firehose

Von Amazon Kinesis Firehose definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDeliveryStream	Gewährt die Berechtigung zum Erstellen eines Bereitstellungsdatenstroms	Schreiben	deliverystream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDeliveryStream	Gewährt die Berechtigung zum Löschen eines Breitstellungsstroms und seiner Daten	Write	deliverystream*		
DescribeDeliveryStream	Gewährt die Berechtigung, den angegebenen Bereitstellungsstrom zu beschreiben und erhält den Status	Lesen	deliverystream*		
ListDeliveryStreams	Gewährt die Berechtigung zum Auflisten Ihrer Bereitstellungsdatenströme	Auflisten			
ListTagsForDeliveryStream	Gewährt die Berechtigung zum Auflisten der Tags für den angegebenen Bereitstellungsdatenstrom	Auflisten	deliverystream*		
PutRecord	Gewährt die Berechtigung zum Schreiben eines einzelnen Datensatzes in einen Amazon Kinesis	Schreiben	deliverystream*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Firehose Bereitstellungsdatenstrom				
PutRecordBatch	Gewährt die Berechtigung zum Schreiben mehrerer Datensätze in einen Bereitstellungsdatenstrom in einem einzigen Aufruf, was einen höheren Durchsatz pro Produzent als beim Schreiben einzelner Datensätze erzielen kann	Schreiben	deliverystream*		
StartDeliveryStreamEncryption	Gewährt die Berechtigung zum Aktivieren der serverseitigen Verschlüsselung (SSE) für den Bereitstellungsdatenstrom	Schreiben	deliverystream*		
StopDeliveryStreamEncryption	Gewährt die Berechtigung zum Deaktivieren des angegebenen Ziels des angegebenen Bereitstellungsdatenstroms	Schreiben	deliverystream*		
TagDeliveryStream	Gewährt die Berechtigung zum Hinzufügen oder Aktualisieren von Tags für den angegebenen Bereitstellungsdatenstrom	Markierung	deliverystream*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagDeliveryStream	Gewährt die Berechtigung zum Entfernen von Tags aus dem angegebenen Bereitstellungsdatenstrom	Markierung	deliverystream*		
				aws:TagKeys	
UpdateDestination	Gewährt die Berechtigung zum Aktualisieren des angegebenen Ziels des angegebenen Bereitstellungsdatenstroms	Schreiben	deliverystream*		

Von Amazon Kinesis Firehose definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
deliverystream	`arn:${Partition}:firehose:${Region}:${Account}:deliverystream/${DeliveryStreamName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Kinesis Firehose

Amazon Kinesis Firehose definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf den Markierungen, die in der Anforderung übergeben werden.	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf den Markierungen, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert Aktionen basierend auf den Tag-Schlüsseln, die in der Anforderung übergeben werden.	ArrayOfString

Aktionen, Ressourcen und Bedingungskontextschlüssel für Amazon Kinesis Video Streams

Amazon Kinesis Video Streams (Servicepräfix: `kinesisvideo`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Kinesis Video Streams definierte Aktionen
- Von Amazon Kinesis Video Streams definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Kinesis Video Streams

Von Amazon Kinesis Video Streams definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ConnectAsMaster	Gewährt die Berechtigung, sich als Master mit dem durch den Endpunkt festgelegten Signalisierungskanal zu verbinden	Write	channel*		
ConnectAsViewer	Gewährt die Berechtigung, sich als Betrachter mit dem vom Endpunkt angegebenen Signalisierungskanal zu verbinden	Write	channel*		
CreateSignalingChannel	Gewährt die Berechtigung, einen Signalisierungskanal zu erstellen	Write	channel*		
				aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
CreateStream	Gewährt die Berechtigung, einen Kinesis-Videostream zu erstellen	Schreiben	stream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteEdgeConfiguration	Gewährt die Berechtigung, die Edge-Konfiguration Ihres Kinesis-Videostreams zu löschen	Schreiben	stream*		
DeleteSignalingChannel	Gewährt die Berechtigung zum Löschen eines bestehenden Signalisierungskanals	Write	channel*		
DeleteStream	Gewährt die Berechtigung, einen vorhandenen Kinesis-Videostream zu löschen	Schreiben	stream*		
DescribeEdgeConfiguration	Gewährt die Berechtigung zum Beschreiben der Edge-Konfiguration Ihres Kinesis-Videostreams	Lesen	stream*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeImageGenerationConfiguration	Gewährt die Berechtigung zum Beschreiben der Konfiguration der Image-Erzeugung Ihres Kinesis-Videostreams	Lesen	stream*		
DescribeMappedResourceConfiguration	Gewährt die Berechtigung, die dem Kinesis-Videostream zugeordnete Ressource zu beschreiben	Auflisten	stream*		
DescribeMediaStorageConfiguration	Gewährt die Berechtigung zum Beschreiben der Medienspeicherkonfiguration eines Signalkanals	Lesen	channel*		
DescribeNotificationConfiguration	Erteilung der Berechtigung zur Beschreibung der Benachrichtigungskonfiguration Ihres Kinesis-Videostreams	Lesen	stream*		
DescribeSignalingChannel	Gewährt die Berechtigung, den angegebenen Signalisierungskanal zu beschreiben	List	channel*		
DescribeStream	Gewährt die Berechtigung, den angegebenen Kinesis-Videostream zu beschreiben	List	stream*		
GetClip	Gewährt die Berechtigung zum Abrufen eines Medienclips aus einem Videostream	Read	stream*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDASHStreamingSessionURL	Gewährt die Berechtigung, eine URL für MPEG-DASH-Videostreaming zu erstellen	Read	stream*		
GetDataEndpoint	Gewährt die Berechtigung, einen Endpunkt für einen bestimmten Stream zu erhalten, um Mediendaten bei Kinesis Video Streams entweder zu lesen oder zu schreiben	Read	stream*		
GetHLSStreamingSessionURL	Gewährt die Berechtigung, eine URL für HLS-Video streaming zu erstellen	Read	stream*		
GetIceServerConfig	Gewährt die Berechtigung, die ICE-Server-Konfiguration zu erhalten	Lesen	channel*		
GetImages	Gewährt die Berechtigung zum Abrufen generierter Images aus Ihrem Kinesis-Videostream	Lesen	stream*		
GetMedia	Gewährt die Berechtigung, Medieninhalte eines Kinesis Video Streams zurückzugeben	Read	stream*		
GetMediaForFragmentList	Gewährt die Berechtigung, Mediendaten nur aus dem persistenten Speicher zu lesen und zurückzugeben	Read	stream*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetSignalingChannelEndpoint	Gewährt die Berechtigung, Endpunkte für eine bestimmte Kombination aus Protokoll und Rolle für einen Signalisierungskanal zu erhalten	Lesen	channel*		
JoinStorageSession	Gewährt die Berechtigung zur Teilnahme an einer Speichersitzung für einen Kanal	Schreiben	channel*		
ListEdgeAgentConfigurations	Gewährt die Berechtigung, die Konfiguration eines Edge-Agents aufzulisten	Auflisten			
ListFragments	Gewährt die Berechtigung, die Fragmente aus dem Archivspeicher basierend auf dem Paginierungs-Token oder dem Selektortyp mit angegebenem Bereich aufzulisten	List	stream*		
ListSignalingChannels	Gewährt die Berechtigung, Ihre Signalisierungskanäle aufzulisten	List			
ListStreams	Gewährt die Berechtigung, Ihre Kinesis Video Streams aufzulisten	List			
ListTagsForResource	Gewährt die Berechtigung, die mit Ihrer Ressource verknüpften Tags abzurufen	Read	channel		
			stream		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForStream	Gewährt die Berechtigung, die mit dem Kinesis-Videostream verknüpften Tags abzurufen	Read	stream*		
PutMedia	Gewährt die Berechtigung, Mediendaten an einen Kinesis-Videostream zu senden	Write	stream*		
SendAlexaOfferToMaster	Gewährt die Berechtigung, das Alexa SDP-Angebot an den Master zu senden	Schreiben	channel*		
StartEdgeConfigurationUpdate	Gewährt die Berechtigung zum Starten des Edge-Konfigurationsupdates Ihres Kinesis-Videostreams	Schreiben	stream*		
TagResource	Gewährt die Berechtigung, einen Satz von Tags an Ihre Ressource anzuhängen	Markieren	channel		
			stream		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagStream	Gewährt die Berechtigung, einen Satz Tags an Ihre Kinesis Video Streams anzuhängen	Markieren	stream*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung, ein oder mehrere Tags aus Ihrer Ressource zu entfernen	Markieren	channel		
			stream		
				aws:TagKeys	
UntagStream	Gewährt die Berechtigung, einen oder mehrere Tags aus Ihren Kinesis Video Streams zu entfernen	Markieren	stream*		
				aws:TagKeys	
UpdateDataRetention	Gewährt die Berechtigung zur Aktualisierung der Datenspeicherungsdauer Ihres Kinesis Video Streams	Schreiben	stream*		
UpdateImageGenerationConfiguration	Gewährt die Berechtigung zum Aktualisieren der Konfiguration der Image-Erzeugung Ihres Kinesis-Videostreams	Schreiben	stream*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateMediaStorageConfiguration	Gewährt die Berechtigung zum Erstellen oder Aktualisieren einer Zuordnung zwischen einem Signalkanal und einem Stream	Schreiben	channel*		
UpdateNotificationConfiguration	Erteilung der Berechtigung zur Aktualisierung der Benachrichtigungskonfiguration Ihres Kinesis-Videostreams	Schreiben	stream*		
UpdateSignalingChannel	Gewährt die Berechtigung, einen bestehenden Signalisierungskanal zu aktualisieren	Write	channel*		
UpdateStream	Gewährt die Berechtigung, einen bestehenden Kinesis-Videostream zu aktualisieren	Write	stream*		

Von Amazon Kinesis Video Streams definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
stream	`arn:${Partition}:kinesisvideo:${Region}:${Account}:stream/${StreamName}/${CreationTime}`	aws:ResourceTag/${TagKey}
channel	`arn:${Partition}:kinesisvideo:${Region}:${Account}:channel/${ChannelName}/${CreationTime}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Kinesis Video Streams

Amazon Kinesis Video Streams definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Anfragen basierend auf den zulässigen Werten für jedes der Tags	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf dem mit dem Stream verknüpften Tag-Wert	Zeichenfolge
aws:TagKeys	Filtert Anfragen basierend auf dem Vorhandensein obligatorischer Tag-Schlüssel in der Anfrage	ArrayOfString

Aktionen, Ressourcen und Zustandsschlüssel für AWS Lake Formation

AWS Lake Formation (Servicepräfix: `lakeformation`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Aktionen, die durch AWS Lake Formation definiert sind

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddLFTagsToResource	Gewährt die Berechtigung zum Anfügen von Lake-Formation-Tags an Katalogressourcen	Tagging			
BatchGrantPermissions	Gewährt Data-Lake-Berechtigungen für einen oder mehrere Prinzipale in einem Batch	Berechtigungsverwaltung			
BatchRevokePermissions	Gewährt die Berechtigung zum Widerrufen von Data-Lake-Berechtigungen von	Berechtigungsverwaltung			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	einem oder mehrerer Prinzipale in einem Batch				
CancelTransaction	Gewährt die Berechtigung zum Abbrechen der angegebenen Transaktion	Schreiben			
CommitTransaction	Gewährt die Berechtigung einen Commit für die angegebene Transaktion auszuführen	Schreiben			
CreateDataCellsFilter	Gewährt die Berechtigung zum Erstellen eines Lake-Formation-Datenzellenfilters	Schreiben			
CreateLFTag	Gewährt die Berechtigung zum Erstellen eines Lake-Formation-Tags	Schreiben			
CreateLakeFormationIdentityCenterConfiguration	Gewährt die Berechtigung zum Erstellen einer IAM-Identity-Center-Verbindung mit Lake Formation, um IAM-Identity-Center-Benutzern und -Gruppen den Zugriff auf Data-Catalog-Ressourcen zu ermöglichen	Schreiben			
CreateLakeFormationOptIn	Lake-Formation-Berechtigungen für die angegebenen Datenbanken, Tabellen und Prinzipale erzwingen	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteDataCellsFilter	Gewährt die Berechtigung zum Löschen eines Lake-Formation-Datenzellenfilters	Schreiben			
DeleteLFTag	Gewährt die Berechtigung zum Löschen eines Lake-Formation-Tags	Schreiben			
DeleteLakeFormationIdentityCenterConfiguration	Gewährt die Berechtigung zum Löschen einer IAM-Identity-Center-Verbindung mit Lake Formation	Schreiben			
DeleteLakeFormationOptIn	Erzwingungen von Lake-Formation-Berechtigungen für die angegebenen Datenbanken, Tabellen und Prinzipale entfernen	Schreiben			
DeleteObjectsOnCancel	Gewährt die Berechtigung zum Löschen der angegebenen Objekte, wenn die Transaktion abgebrochen wird	Schreiben			
DeregisterResource	Gewährt die Berechtigung zum Aufheben der Registrierung eines registrierten Standorts	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeLakeFormationIdentityCenterConfiguration	Gewährt die Berechtigung zum Beschreiben der IAM-Identity-Center-Verbindung mit Lake Formation	Lesen			
DescribeResource	Gewährt die Berechtigung, einen registrierten Standort zu beschreiben	Lesen			
DescribeTransaction	Gewährt die Berechtigung, den Status für die angegebene Transaktion abzurufen	Lesen			
ExtendTransaction	Gewährt die Berechtigung, das Zeitlimit für die angegebene Transaktion zu verlängern	Schreiben			
GetDataAccess	Gewährt Zugriffsberechtigungen für virtuelle Data-Lake.	Schreiben			
GetDataCellsFilter	Gewährt die Berechtigung zum Abrufen eines Lake-Formation-Datenzellenfilters	Lesen			
GetDataLakeSettings	Gewährt die Berechtigung zum Abrufen von Data-Lake-Einstellungen wie der Liste der Data-Lake-Administratoren und Datenbank- und Tabellenstandardberechtigungen	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetEffectivePermissionsForPath	Gewährt die Berechtigung zum Abrufen von Berechtigungen, die Ressourcen im angegebenen Pfad zugeordnet sind	Lesen			
GetLFTag	Gewährt die Berechtigung zum Abrufen eines Lake-Formation-Tags	Lesen			
GetQueryState	Gewährt die Berechtigung zum Abrufen des Status der angegebenen Abfrage	Lesen			lakeformation:StartQueryPlanning
GetQueryStatistics	Gewährt die Berechtigung zum Abrufen der Statistik der angegebenen Abfrage	Lesen			lakeformation:StartQueryPlanning
GetResourceLFTags	Gewährt die Berechtigung zum Abrufen von Lakeformations-Tags auf einer Katalogressource	Lesen			
GetTableObjects	Gewährt die Berechtigung zum Abrufen von Objekten aus einer Tabelle	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetWorkUnitResults	Gewährt die Berechtigung zum Abrufen der Ergebnisse für die angegebenen Arbeitseinheiten	Lesen			lakeformation:GetWorkUnits lakeformation:StartQueryPlanning
GetWorkUnits	Gewährt die Berechtigung zum Abrufen der Arbeitseinheiten für die angegebenen Abfragen	Lesen			lakeformation:StartQueryPlanning
GrantPermissions	Gewährt einem Prinzipal die Berechtigung für Data-Lake-Berechtigungen	Berechtigungsverwaltung			
ListDataCellsFilter	Gewährt die Berechtigung zum Auflisten von Zellenfiltern	Auflisten			
ListLFTags	Gewährt die Berechtigung zum Auflisten von Lake-Formation-Tags	Lesen			
ListLakeFormationOptIns	Aktuelle Liste der Ressourcen und Prinzipale abrufen, die sich für die Erzwingung der Lake-Formation-Berechtigungen entschieden haben	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListPermissions	Gewährt die Berechtigung zum Auflisten von Berechtigungen, die nach Prinzipal oder Ressource gefiltert sind	Auflisten			
ListResources	Gewährt die Berechtigung zum Auflisten registrierter Standorte	Auflisten			
ListTableStorageOptimizers	Gewährt die Berechtigung zum Auflisten aller Speicheroptimierer für die verwaltete Tabelle	Auflisten			
ListTransactions	Gewährt die Berechtigung zum Auflisten aller Transaktionen im System	Auflisten			
PutDataLakeSettings	Gewährt die Berechtigung zum Überschreiben von Data-Lake-Einstellungen wie der Liste der Data-Lake-Administratoren und Datenbank- und Tabellenstandardberechtigungen	Berechtigungsverwaltung			
RegisterResource	Gewährt die Berechtigung, einen neuen Standort zu registrieren, der von Lake Formation verwaltet werden soll	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RemoveLFTagsFromResource	Gewährt die Berechtigung zum Entfernen von Lakeformations-Tags aus Katalogressourcen	Tagging			
RevokePermissions	Gewährt die Berechtigung zum Widerrufen von Data-Lake-Berechtigungen von einem Prinzipal	Berechtigungsverwaltung			
SearchDatabasesByLFTags	Gewährt die Berechtigung zum Auflisten von Katalogdatenbanken mit Lake-Formation-Tags	Lesen			
SearchTablesByLFTags	Gewährt die Berechtigung zum Auflisten von Katalogtabellen mit Lake-Formation-Tags	Lesen			
StartQueryPlanning	Gewährt die Berechtigung zum Initiieren der Planung der gegebenen Abfrage	Schreiben			
StartTransaction	Gewährt die Berechtigung zum Starten einer neuen Transaktion	Schreiben			
UpdateDataCellsFilter	Gewährt die Berechtigung zum Aktualisieren eines Lake-Formation-Datenzellenfilters	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateLFTag	Gewährt die Berechtigung zum Aktualisieren eines Lake-Formation-Tags	Schreiben			
UpdateLakeFormationIdentityCenterConfiguration	Gewährt die Berechtigung zum Aktualisieren der IAM-Identity-Center-Verbindungsparameter	Schreiben			
UpdateResource	Gewährt die Berechtigung, einen registrierten Standort zu aktualisieren	Schreiben			
UpdateTableObjects	Gewährt die Berechtigung zum Hinzufügen oder Löschen der angegebenen Objekte zu oder aus einer Tabelle	Schreiben			
UpdateTableStorageOptimizer	Gewährt die Berechtigung zum Aktualisieren der Konfiguration des Speicheroptimierers für die verwaltete Tabelle	Schreiben			

Ressourcentypen definiert durch AWS Lake Formation

AWS Lake Formation unterstützt nicht die Angabe eines Ressourcen-ARN in einem `Resource` Element einer IAM-Richtlinie. Um den Zugang zu AWS Lake Formation zu ermöglichen, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Lake Formation

Lake Formation hat keine servicespezifischen Kontextschlüssel, die im `Condition` Element der Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS-Lambda

AWS Lambda (Servicepräfix: `lambda`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Lambda definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich

sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddLayerVersionPermission	Gewährt die Berechtigung zum Hinzufügen von Berechtigungen zur ressourcenbasierten Richtlinie einer Version einer AWS Lambda-Ebene	Berechtigungsverwaltung	layerVersion*		
AddPermission	Gewährt die Berechtigung, einem AWS-Service oder einem anderen Konto die Berechtigung zur Verwendung	Berechtigungsverwaltung	function*	lambda:Principal	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	einer AWS-Lambda-Funktion zu erteilen			lambda:FunctionUrlAuthType	
CreateAlias	Gewährt die Berechtigung zum Erstellen eines Alias für eine Lambda-Funktionsversion	Write	function*		
CreateCodeSigningConfig	Gewährt die Berechtigung zum Erstellen einer Code-Signierungskonfiguration für AWS Lambda	Write			
CreateEventSourceMapping	Gewährt die Berechtigung zum Erstellen eines Mappings zwischen einer Ereignisquelle und einer AWS-Lambda-Funktion	Write		lambda:FunctionArn	
CreateFunction	Gewährt die Berechtigung zum Erstellen einer AWS-Lambda-Funktion	Schreiben	function*		iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				lambda:Layer lambda:VpcIds lambda:SubnetIds lambda:SecurityGroupIds lambda:CodeSigningConfigArn aws:RequestTag/${TagKey} aws:TagKeys	
CreateFunctionUrlConfig	Gewährt die Berechtigung zum Erstellen einer Funktions-URL-Konfiguration für eine Lambda-Funktion	Schreiben	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteAlias	Gewährt die Berechtigung zum Löschen eines AWS-Lambda-Funktionsalias	Write	function*		
DeleteCodeSigningConfig	Gewährt die Berechtigung zum Löschen einer Code-Signierungskonfiguration für AWS Lambda	Write	codesigningconfig*		
DeleteEventSourceMapping	Gewährt die Berechtigung zum Löschen eines AWS-Lambda-Ereignisquellenmappings	Write	eventSourceMapping*		
				lambda:FunctionArn	
DeleteFunction	Gewährt die Berechtigung zum Löschen einer AWS-Lambda-Funktion	Write	function*		
DeleteFunctionCodeSigningConfig	Gewährt die Berechtigung zum Trennen einer Code-Signierungskonfiguration von einer AWS-Lambda-Funktion	Write	function*		
DeleteFunctionConcurrency	Gewährt die Berechtigung, ein Limit für die gleichzeitige Ausführung aus einer AWS-Lambda-Funktion zu entfernen	Write	function*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteFunctionEventInvokeConfig	Gewährt die Berechtigung zum Löschen der Konfiguration für den asynchronen Aufruf für eine Funktion, eine Version oder einen Alias in AWS Lambda	Schreiben	function*		
DeleteFunctionUrlConfig	Gewährt die Berechtigung zum Löschen einer Funktions-URL-Konfiguration für eine Lambda-Funktion	Schreiben	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	
DeleteLayerVersion	Gewährt die Berechtigung zum Löschen einer Version einer AWS-Lambda-Ebene	Write	layerVersion*		
DeleteProvisionedConcurrencyConfig	Gewährt die Berechtigung zum Löschen der bereitgestellten Parallelitätskonfiguration für eine AWS-Lambda-Funktion	Write	function alias		
			function version		
DisableReplication [nur Berechtigung]	Gewährt die Berechtigung zum Deaktivieren der Replikation für eine Lambda @Edge-Funktion	Berechtigungsverwaltung	function*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
EnableReplication [nur Berechtigung]	Gewährt die Berechtigung zum Aktivieren der Replikation für eine Lambda @Edge-Funktion	Berechtigungsverwaltung	function*		
GetAccountSettings	Gewährt die Berechtigung zum Anzeigen von Details zu den Beschränkungen und der Nutzung eines Kontos in einer AWS-Region	Read			
GetAlias	Gewährt die Berechtigung zum Anzeigen von Details zu einem AWS-Lambda-Funktionsalias	Read	function*		
GetCodeSigningConfig	Gewährt die Berechtigung zum Anzeigen von Details zu einer Code-Signierungskonfiguration für AWS Lambda	Read	code signing config*		
GetEventSourceMapping	Gewährt die Berechtigung zum Anzeigen von Details zu einem AWS-Lambda-Ereignisquellenmapping	Read	eventSourceMapping*		
				lambda:FunctionArn	
GetFunction	Gewährt die Berechtigung zum Anzeigen von Details zu einer AWS-Lambda-Funktion	Read	function*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetFunctionCodeSigningConfig	Gewährt die Berechtigung zum Anzeigen des Code-Signierungskonfigurations-ARNs, der einer AWS-Lambda-Funktion angefügt ist	Read	function*		
GetFunctionConcurrency	Gewährt die Berechtigung zum Anzeigen von Details zur reservierten Parallelitätskonfiguration für eine Funktion	Read	function*		
GetFunctionConfiguration	Gewährt die Berechtigung zum Anzeigen von Details zu den versionsspezifischen Einstellungen einer AWS-Lambda-Funktion oder -Version	Read	function*		
GetFunctionEventInvokeConfig	Gewährt die Berechtigung zum Anzeigen der Konfiguration für den asynchronen Aufruf für eine Funktion, Version oder einen Alias	Lesen	function*		
GetFunctionUrlConfig	Gewährt die Berechtigung zum Lesen einer Funktions-URL-Konfiguration für eine Lambda-Funktion	Lesen	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetLayerVersion	Gewährt die Berechtigung zum Anzeigen von Details zu einer Version einer AWS-Lambda-Ebene. Beachten Sie, dass diese Aktion auch die GetLayerVersionByArn-API unterstützt	Read	layerVersion*		
GetLayerVersionPolicy	Gewährt die Berechtigung zum Anzeigen der ressourcenbasierten Richtlinie für eine Version einer AWS-Lambda-Ebene	Read	layerVersion*		
GetPolicy	Gewährt die Berechtigung zum Anzeigen der ressourcenbasierten Richtlinie für eine Funktion, eine Version oder ein Alias in AWS Lambda	Read	function*		
GetProvisionedConcurrencyConfig	Gewährt die Berechtigung zum Anzeigen der bereitgestellten Parallelitätskonfiguration für den Alias oder die Version einer AWS-Lambda-Funktion	Lesen	function alias		
			function version		
GetRuntimeManagementConfig	Gewährt die Berechtigung zum Anzeigen der Laufzeitverwaltungskonfiguration einerAWS-Lambda-Funktion	Lesen	function*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
InvokeAsync	Gewährt die Berechtigung, eine Funktion asynchron aufzurufen (Veraltet)	Schreiben	function*		
InvokeFunction	Gewährt die Berechtigung zum Aufrufen einer AWS-Lambda-Funktion	Schreiben	function*		
				lambda:EventSourceToken	
InvokeFunctionUrl [nur Berechtigung]	Gewährt die Berechtigung zum Aufrufen einer AWS-Lambda-Funktion per URL	Schreiben	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn lambda:EventSourceToken	
ListAliases	Gewährt die Berechtigung zum Abrufen einer Liste von Aliasen für eine AWS-Lambda-Funktion	List	function*		
ListCodeSigningConfigs	Gewährt die Berechtigung zum Abrufen einer Liste von Code-Signierungskonfigurationen für AWS Lambda	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListEventSourceMappings	Gewährt die Berechtigung zum Abrufen einer Liste von AWS-Lambda-Ereignisquellenmappings	List			
ListFunctionEventInvokeConfigs	Gewährt die Berechtigung zum Abrufen einer Liste von Konfigurationen für den asynchronen Aufruf für eine Funktion	Auflisten	function*		
ListFunctionUrlConfigs	Gewährt die Berechtigung zum Lesen einer Funktions-URL-Konfiguration für eine Funktion	Auflisten	function*		
				lambda:FunctionUrlAuthType	
ListFunctions	Gewährt die Berechtigung zum Abrufen einer Liste der AWS-Lambda-Funktionen mit der versionsspezifischen Konfiguration jeder Funktion	List			
ListFunctionsByCodeSigningConfig	Gewährt die Berechtigung zum Abrufen einer Liste der AWS-Lambda-Funktionen anhand der zugewiesenen Code-Signierungskonfiguration	List	code signing config*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListLayerVersions	Gewährt die Berechtigung zum Abrufen einer Liste von Versionen einer AWS-Lambda-Ebene	List			
ListLayers	Gewährt die Berechtigung zum Abrufen einer Liste von AWS-Lambda-Ebenen mit Details zur neuesten Version der einzelnen Ebenen	List			
ListProvisionedConcurrencyConfigs	Gewährt die Berechtigung zum Abrufen einer Liste bereitgestellter Parallelitätskonfigurationen für eine AWS-Lambda-Funktion	List	function*		
ListTags	Gewährt die Berechtigung zum Abrufen einer Liste von Tags für eine AWS-Lambda-Funktion	Read	function*		
ListVersionsByFunction	Gewährt die Berechtigung zum Abrufen einer Liste von Versionen für eine AWS-Lambda-Funktion	List	function*		
PublishLayerVersion	Gewährt die Berechtigung zum Erstellen einer AWS-Lambda-Ebene	Write	layer*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PublishVersion	Gewährt die Berechtigung zum Erstellen einer AWS-Lambda-Funktionsversion	Write	function*		
PutFunctionCodeSigningConfig	Gewährt die Berechtigung zum Anfügen einer Code-Signierungskonfiguration an eine AWS-Lambda-Funktion	Write	code signing config*		
			function*		
				lambda:CodeSigningConfigArn	
PutFunctionConcurrency	Gewährt die Berechtigung zum Konfigurieren der reservierten Parallelität für eine AWS-Lambda-Funktion	Write	function*		
PutFunctionEventInvokeConfig	Gewährt die Berechtigung zum Konfigurieren von Optionen für den asynchronen Aufruf einer Funktion, einer Version oder eines Alias in AWS Lambda	Write	function*		
PutProvisionedConcurrencyConfig	Gewährt die Berechtigung zum Konfigurieren der bereitgestellten Parallelität für den Alias oder die Version einer AWS-Lambda-Funktion	Schreiben	function alias		
			function version		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutRuntimeManagementConfig	Gewährt die Berechtigung zum Aktualisieren der Laufzeitverwaltungskonfiguration einerAWS-Lambda-Funktion	Schreiben	function*		
RemoveLayerVersionPermission	Gewährt die Berechtigung zum Entfernen einer Anweisung aus der Berechtigungsrichtlinie für eine Version einer AWS-Lambda-Ebene	Berechtigungsverwaltung	layerVersion*		
RemovePermission	Gewährt die Berechtigung zum Widerrufen der Berechtigung zur Funktionsbenutzung von einem AWS-Service oder einem anderen Konto	Berechtigungsverwaltung	function*		
				lambda:Principal lambda:FunctionUrlAuthType	
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer AWS-Lambda-Funktion	Markieren	function*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer AWS-Lambda-Funktion	Markieren	function*		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateAlias	Gewährt die Berechtigung zum Aktualisieren der Konfiguration des Alias einer AWS-Lambda-Funktion	Write	function*		
UpdateCodeSigningConfig	Gewährt die Berechtigung zum Aktualisieren einer Code-Signierungskonfiguration für AWS Lambda	Write	codesigningconfig*		
UpdateEventSourceMapping	Gewährt die Berechtigung zum Aktualisieren der Konfiguration eines AWS-Lambda-Ereignisquellenmappings	Write	eventSourceMapping*		
				lambda:FunctionArn	
UpdateFunctionCode	Gewährt die Berechtigung zum Aktualisieren des Codes einer AWS-Lambda-Funktion	Write	function*		
UpdateFunctionCodeSigningConfig	Gewährt die Berechtigung zum Aktualisieren der Code-Signierungskonfiguration einer AWS-Lambda-Funktion	Write	codesigningconfig*		
			function*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateFunctionConfiguration	Gewährt die Berechtigung zum Ändern der versionsspezifischen Einstellungen einer AWS-Lambda-Funktion	Write	function*		
				lambda:Layer lambda:VpcIds lambda:SubnetIds lambda:SecurityGroupIds	
UpdateFunctionEventInvokeConfig	Gewährt die Berechtigung zum Ändern der Konfiguration für den asynchronen Aufruf für eine Funktion, eine Version oder einen Alias in AWS Lambda	Schreiben	function*		
UpdateFunctionUrlConfig	Gewährt die Berechtigung zum Aktualisieren einer Funktions-URL-Konfiguration für eine Lambda-Funktion	Schreiben	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	

Von AWS Lambda definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
code signing config	`arn:${Partition}:lambda:${Region}:${Account}:code-signing-config:${CodeSigningConfigId}`	
eventSourceMapping	`arn:${Partition}:lambda:${Region}:${Account}:event-source-mapping:${UUID}`	
function	`arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}`	aws:ResourceTag/${TagKey}
function alias	`arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}:${Alias}`	aws:ResourceTag/${TagKey}
function version	`arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}:${Version}`	aws:ResourceTag/${TagKey}
layer	`arn:${Partition}:lambda:${Region}:${Account}:layer:${LayerName}`	
layerVersion	`arn:${Partition}:lambda:${Region}:${Account}:layer:${LayerName}:${LayerVersion}`	

Bedingungsschlüssel für AWS Lambda

AWS Lambda definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString
lambda:CodeSigningConfigArn	Filtert den Zugriff nach dem ARN einer Code-Signierungskonfiguration für AWS Lambda	ARN
lambda:EventSourceToken	Filtert den Zugriff anhand der ID aus einer Nicht–AWS Event-Quelle, die für die AWS Lambda-Funktion konfiguriert ist	Zeichenfolge
lambda:FunctionArn	Filtert den Zugriff nach dem ARN einer AWS-Lambda-Funktion	ARN
lambda:FunctionUrlAuthType	Filtert den Zugriff nach dem in der Anforderung angegebenen Autorisierungstyp. Verfügbar während folgender Vorgänge: CreateFunctionUrlConfig, UpdateFunctionUrlConfig, DeleteFunctionUrlConfig,	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
	GetFunctionUrlConfig, ListFunctionUrlConfig, AddPermission und RemovePermission	
lambda:Layer	Filtert den Zugriff durch den ARN einer AWS Lambda-Ebene	ArrayOfString
lambda:Principal	Filtert den Zugriff, indem Sie den AWS-Service oder das Konto einschränken, das eine Funktion aufrufen kann	Zeichenfolge
lambda:SecurityGroupIds	Filtert den Zugriff nach der ID von Sicherheitsgruppen, die für die AWS-Lambda-Funktion konfiguriert sind	ArrayOfString
lambda:SourceFunctionArn	Filtert den Zugriff nach ARN der AWS-Lambda-Funktion, von dem die Anforderung stammt	ARN
lambda:SubnetIds	Filtert den Zugriff nach der ID von Subnetzen, die für die AWS-Lambda-Funktion konfiguriert sind	ArrayOfString
lambda:VpcIds	Filtert den Zugriff nach der ID der VPC, die für die AWS-Lambda-Funktion konfiguriert ist	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für den AWS Launch Wizard

Der AWS Launch Wizard (Servicepräfix: `launchwizard`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Vom AWS Launch Wizard definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAdditionalNode [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines zusätzlichen Knotens	Schreiben			
CreateDeployment	Gewährt die Berechtigung zum Erstellen einer Bereitstellung	Schreiben			
CreateSettingsSet [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines Satzes von Anwendungseinstellungen	Schreiben			
DeleteAdditionalNode [nur Berechtigung]	Gewährt die Berechtigung zum Löschen eines zusätzlichen Knotens	Schreiben			
DeleteApp [nur Berechtigung]	Gewährt die Berechtigung zum Löschen einer Anwendung	Schreiben			
DeleteDeployment	Erteilt die Berechtigung zum Löschen einer Bereitstellung	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteSettingsSet [nur Berechtigung]	Gewährt die Berechtigung zum Löschen eines Satzes von Einstellungen	Schreiben			
DescribeAdditionalNode [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben eines zusätzlichen Knotens	Lesen			
DescribeProvisionedApp [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben von Bereitstellungsanwendungen	Lesen			
DescribeProvisioningEvents [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben von Bereitstellungsereignissen	Lesen			
DescribeSettingsSet [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben eines Satzes von Anwendungseinstellungen	Lesen			
GetDeployment	Gewährt die Berechtigung zum Abrufen einer Bereitstellung	Lesen			
GetInfrastructureSuggestion [nur Berechtigung]	Gewährt die Berechtigung zum Erhalten eines Infrastrukturvorschlags	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetIpAddress [nur Berechtigung]	Gewährt die Berechtigung zum Erhalten der IP-Adresse eines Kunden	Lesen			
GetResourceCostEstimate [nur Berechtigung]	Gewährt die Berechtigung zum Erhalten von Kostenschätzungen	Lesen			
GetResourceRecommendation [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Empfehlungen für eine Ressource	Lesen			
GetSettingsSet [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen eines Satzes von Einstellungen	Lesen			
GetWorkload	Gewährt die Berechtigung zum Abrufen eines Workloads	Lesen			
GetWorkloadAsset [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Workload-Assets	Lesen			
GetWorkloadAssets [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Workload-Assets	Lesen			
ListAdditionalNodes [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten zusätzlicher Knoten	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAllowedResources [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aller zulässigen Ressourcen	Auflisten			
ListDeploymentEvents	Gewährt die Berechtigung zum Auflisten der Ereignisse, die während einer Bereitstellung aufgetreten sind	Auflisten			
ListDeployments	Gewährt die Berechtigung zum Auflisten von Bereitstellungen	Auflisten			
ListProvisionedApps [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Bereitstellungsanwendungen	Auflisten			
ListResourceCostEstimates [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Kostenschätzungen für Ressourcen	Auflisten			
ListSettingsSets [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Sätzen von Einstellungen	Auflisten			
ListWorkloadDeploymentOptions [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Bereitstellungsoptionen für einen bestimmten Workload	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListWorkloadDeploymentPatterns	Gewährt die Berechtigung zum Auflisten von Bereitstellungsmuster für einen Workload	Auflisten			
ListWorkloads	Gewährt die Berechtigung zum Auflisten von Workloads	Auflisten			
PutSettingsSet [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines Satzes von Einstellungen	Schreiben			
StartProvisioning [nur Berechtigung]	Gewährt die Berechtigung zum Starten einer Bereitstellung	Schreiben			
UpdateSettingsSet [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren eines Satzes von Anwendungseinstellungen	Schreiben			

Von AWS Launch Wizard definierte Ressourcentypen

Der AWS Launch Wizard unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf den AWS Launch Wizard zu ermöglichen, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für den AWS Launch Wizard

Der Startassistent besitzt keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Lex

Amazon Lex (Servicepräfix: `lex`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Lex definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateBotVersion	Erstellt eine neue Version basierend auf der $LATEST-Version des angegebenen Bots	Schreiben	bot version*		
CreateIntentVersion	Erstellt eine neue Version basierend auf der $LATEST-Version der angegebenen Absicht	Schreiben	intent version*		
CreateSlotTypeVersion	Erstellt eine neue Version basierend auf der $LATEST-Version des angegebenen Slot-Typs	Schreiben	slottype version*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteBot	Löscht alle Versionen eines Bots	Schreiben	bot version*		
DeleteBotAlias	Löscht einen Alias für den angegebenen Bot	Schreiben	bot alias*		
DeleteBotChannelAssociation	Löscht das Mapping zwischen dem Alias eines Amazon-Lex-Bots und einer Messaging-Plattform	Schreiben	channel*		
DeleteBotVersion	Löscht eine bestimmte Version eines Bots	Schreiben	bot version*		
DeleteIntent	Löscht alle Versionen einer Absicht	Schreiben	intent version*		
DeleteIntentVersion	Löscht eine bestimmte Version einer Absicht	Schreiben	intent version*		
DeleteSession	Entfernt Sitzungsinformationen für einen angegebenen Bot, Alias und eine Benutzer-ID	Schreiben	bot alias		
			bot version		
DeleteSlotType	Löscht alle Versionen eines Slot-Typs	Schreiben	slottype version*		
DeleteSlotTypeVersion	Löscht eine bestimmte Version eines Slot-Typs	Schreiben	slottype version*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteUtterances	Löscht die Informationen, die Amazon Lex für Äußerungen auf einem bestimmten Bot und mit einer bestimmten userId verwaltet	Schreiben	bot version*		
GetBot	Gibt Informationen für einen bestimmten Bot zurück. Neben dem Bot-Namen muss die Bot-Version oder der Bot-Alias angegeben werden	Lesen	bot alias		
			bot version		
GetBotAlias	Gibt Informationen zu einem Amazon-Lex-Bot-Alias zurück	Lesen	bot alias*		
GetBotAliases	Gibt eine Liste der Alias für einen bestimmten Amazon-Lex-Bot zurück	Auflisten			
GetBotChannelAssociation	Gibt Informationen zum Mapping zwischen dem Alias eines Amazon-Lex-Bots und einer Messaging-Plattform zurück	Lesen	channel*		
GetBotChannelAssociations	Gibt eine Liste aller Channels zurück, die einem einzelnen Bot zugeordnet sind	Auflisten	channel*		
GetBotVersions	Gibt Informationen zu allen Versionen eines bestimmten Bots zurück	Auflisten	bot version*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBots	Gibt Informationen zur $LATEST-Version aller Bots zurück, die dem vom Client bereitgestellten Filter entsprechen	Auflisten			
GetBuiltInIntent	Gibt Informationen zu einer integrierten Absicht zurück	Lesen			
GetBuiltInIntents	Ruft eine Liste der integrierten Absichten ab, die den angegebenen Kriterien entsprechen	Lesen			
GetBuiltInSlotTypes	Ruft eine Liste der integrierten Slot-Typen ab, die den angegebenen Kriterien entsprechen	Lesen			
GetExport	Exportiert Amazon-Lex-Ressourcen in einem angeforderten Format	Lesen	bot version*		
GetImport	Ruft Informationen über einen mit StartImport gestarteten Importauftrag ab	Lesen			
GetIntent	Gibt Informationen zu einer bestimmten Absicht zurück. Neben dem Namen muss auch die Version der Absicht angegeben werden	Lesen	intent version*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetIntentVersions	Gibt Informationen zu allen Versionen einer bestimmten Absicht zurück	Auflisten	intent version*		
GetIntents	Gibt Informationen zur $LATEST-Version aller Absichten zurück, die dem vom Client bereitgestellten Filter entsprechen	Auflisten			
GetMigration	Gewährt die Berechtigung zum Anzeigen einer laufenden oder abgeschlossenen Migration	Lesen			
GetMigrations	Gewährt die Berechtigung zum Anzeigen der Liste der Migrationen von Amazon Lex v1 zu Amazon Lex v2	Auflisten			
GetSession	Gibt Sitzungsinformationen für einen angegebenen Bot, Alias und eine Benutzer-ID zurück	Lesen	bot alias		
			bot version		
GetSlotType	Gibt Informationen hinsichtlich einer bestimmten Version eines Slot-Typs zurück. Neben dem Namen muss auch die Version des Slot-Typs angegeben werden	Lesen	slottype version*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetSlotTypeVersions	Gibt Informationen zu allen Versionen eines bestimmten Slot-Typs zurück	Auflisten	slottype version*		
GetSlotTypes	Gibt Informationen zur $LATEST-Version aller Slot-Typen zurück, die dem vom Client bereitgestellten Filter entsprechen	Auflisten			
GetUtterancesView	Gibt eine Ansicht der aggregierten Äußerungsdaten für Versionen eines Bots in einem aktuellen Zeitraum zurück	Auflisten	bot version*		
ListTagsForResource	Listet Tags für eine Lex-Ressource auf	Lesen	bot		
			bot alias		
			channel		
PostContent	Sendet eine Benutzereingabe (Text oder Sprache) an Amazon Lex	Schreiben	bot alias		
			bot version		
PostText	Sendet eine Benutzereingabe (nur Text) an Amazon Lex	Schreiben	bot alias		
			bot version		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutBot	Erstellt oder aktualisiert die $LATEST-Version eines Amazon-Lex-Konversations-Bots	Schreiben	bot version*		
				aws:TagKeys aws:RequestTag/${TagKey}	
PutBotAlias	Erstellt oder aktualisiert einen Alias für einen bestimmten Bot	Schreiben	bot alias*		
				aws:TagKeys aws:RequestTag/${TagKey}	
PutIntent	Erstellt oder aktualisiert die $LATEST-Version einer Absicht	Schreiben	intent version*		
PutSession	Erstellt eine neue Sitzung oder ändert eine bestehende Sitzung mit einem Amazon-Lex-Bot	Schreiben	bot alias		
			bot version		
PutSlotType	Erstellt oder aktualisiert die $LATEST-Version eines Slot-Typs	Schreiben	slottype version*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartImport	Startet einen Auftrag zum Importieren einer Ressource in Amazon Lex	Schreiben			
StartMigration	Gewährt die Berechtigung, einen Bot von Amazon Lex v1 zu Amazon Lex v2 zu migrieren	Schreiben	bot version*		
TagResource	Fügt Tags zu einer Lex-Ressource hinzu oder überschreibt sie	Markieren	bot		
			bot alias		
			channel		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Entfernt Tags aus einer Lex-Ressource	Markieren	bot		
			bot alias		
			channel		
				aws:TagKeys aws:RequestTag/${TagKey}	

Von Amazon Lex definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
bot	`arn:${Partition}:lex:${Region}:${Account}:bot:${BotName}`	aws:ResourceTag/${TagKey}
bot version	`arn:${Partition}:lex:${Region}:${Account}:bot:${BotName}:${BotVersion}`	aws:ResourceTag/${TagKey}
bot alias	`arn:${Partition}:lex:${Region}:${Account}:bot:${BotName}:${BotAlias}`	aws:ResourceTag/${TagKey}
channel	`arn:${Partition}:lex:${Region}:${Account}:bot-channel:${BotName}:${BotAlias}:${ChannelName}`	aws:ResourceTag/${TagKey}
intent version	`arn:${Partition}:lex:${Region}:${Account}:intent:${IntentName}:${IntentVersion}`	
slottype version	`arn:${Partition}:lex:${Region}:${Account}:slottype:${SlotName}:${SlotVersion}`	

Bedingungsschlüssel für Amazon Lex

Amazon Lex definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen

zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den Tags in der Anforderung.	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff über die Tags, die einer Lex-Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf dem Satz von Tag-Schlüsseln in der Anforderung	ArrayOfString
lex:associatedIntents	Ermöglicht das Steuern des Zugriffs basierend auf in der Anforderung enthaltenen Absichten	ArrayOfString
lex:associatedSlotTypes	Ermöglicht das Steuern des Zugriffs basierend auf in der Anforderung enthaltenen Slot-Typen	ArrayOfString
lex:channelType	Ermöglicht das Steuern des Zugriffs basierend auf in der Anforderung enthaltenen Channel-Typen	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Lex V2

Amazon Lex V2 (Servicepräfix: `lex`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.

- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Lex V2 definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWSzu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchCreateCustomVocabularyItem	Gewährt die Berechtigung, neue Elemente in einem bestehenden benutzerdefinierten Vokabular zu erstellen	Schreiben	bot*		
BatchDeleteCustomVocabularyItem	Gewährt die Berechtigung zum Löschen von vorhandenen Elementen in einem vorhandenen benutzerdefinierten Vokabular	Schreiben	bot*		
BatchUpdateCustomVocabularyItem	Gewährt die Berechtigung zum Aktualisieren von bestehenden Elementen in einem benutzerdefiniertem Vokabular	Schreiben	bot*		
BuildBotLocale	Gewährt die Berechtigung zum Erstellen einer bestehenden Bot-Locale in einem Bot	Write	bot*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateBot	Gewährt die Berechtigung zum Erstellen eines neuen Bots und eines Testbot-Alias, der auf die DRAFT-Bot-Version verweist	Write	bot*		
			bot alias*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateBotAlias	Gewährt die Berechtigung zum Erstellen eines neuen Bot-Alias in einem Bot	Write	bot alias*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateBotChannel [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines Bot-Channels in einem bestehenden Bot	Write	bot*		
CreateBotLocale	Gewährt die Berechtigung zum Erstellen einer neuen Bot-Locale in einem bestehenden Bot	Schreiben	bot*		
CreateBotReplica	Gewährt die Berechtigung zum Erstellen eines Bot-Replikats für einen Bot	Schreiben	bot*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateBotVersion	Gewährt die Berechtigung zum Erstellen einer neuen Version eines bestehenden Bots	Schreiben	bot*		
CreateCustomVocabulary [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen von neuem benutzerdefiniertem Vokabular in einer bestehenden Bot-Locale	Schreiben	bot*		
CreateExport	Gewährt die Berechtigung zum Erstellen eines Exports für eine vorhandene Ressource	Write	bot		
			test set		
CreateIntent	Gewährt die Berechtigung zum Erstellen einer neuen Absicht in einer bestehenden Bot-Locale	Write	bot*		
CreateResourcePolicy	Gewährt die Berechtigung zum Erstellen einer neuen Ressourcenrichtlinie für eine Lex-Ressource	Write	bot		
			bot alias		
CreateSlot	Gewährt die Berechtigung zum Erstellen eines neuen Slots in einer Absicht	Write	bot*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSlotType	Gewährt die Berechtigung zum Erstellen eines neuen Slot-Typs in einer vorhandenen Bot-Locale	Schreiben	bot*		
CreateTestSet [nur Berechtigung]	Gewährt die Berechtigung, einen neuen Testsatz zu importieren	Schreiben			
CreateTestSetDiscrepancyReport	Gewährt die Berechtigung, einen Bericht über Testsatzunstimmigkeiten zu erstellen	Schreiben	test set*		
CreateUploadUrl	Gewährt die Berechtigung zum Erstellen einer Upload-URL für die Importdatei	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteBot	Gewährt die Berechtigung zum Löschen eines bestehenden Bots	Write	bot*		lex:DeleteBotAlias lex:DeleteBotChannel lex:DeleteBotLocale lex:DeleteBotVersion lex:DeleteIntent lex:DeleteSlot lex:DeleteSlotType
			bot alias*		
DeleteBotAlias	Gewährt die Berechtigung zum Löschen eines bestehenden Bot-Alias in einem Bot	Write	bot alias*		
DeleteBotChannel [nur Berechtigung]	Gewährt die Berechtigung zum Löschen eines bestehenden Bot-Channels	Write	bot*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteBotLocale	Gewährt die Berechtigung zum Löschen einer vorhandenen Bot-Locale in einem Bot	Schreiben	bot*		lex:DeleteIntent lex:DeleteSlot lex:DeleteSlotType
DeleteBotReplica	Gewährt die Berechtigung zum Löschen eines vorhandenen Bot-Replikats	Schreiben	bot*		
DeleteBotVersion	Gewährt die Berechtigung zum Löschen einer bestehenden Bot-Version	Schreiben	bot*		
DeleteCustomVocabulary	Gewährt die Berechtigung zum Löschen von neuem benutzerdefiniertem Vokabular in einer Bot-Locale	Schreiben	bot*		
DeleteExport	Gewährt die Berechtigung zum Löschen eines bestehenden Exports	Write	bot		
			test set		
DeleteImport	Gewährt die Berechtigung zum Löschen eines bestehenden Imports	Write	bot		
			test set		
DeleteIntent	Gewährt die Berechtigung zum Löschen einer bestehenden Absicht in einer Bot-Locale	Write	bot*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteResourcePolicy	Gewährt die Berechtigung zum Löschen einer bestehenden Ressourcenrichtlinie für eine Lex-Ressource	Write	bot		
			bot alias		
DeleteSession	Gewährt die Berechtigung zum Löschen von Sitzungsinformationen für einen Bot-Alias und eine Benutzer-ID	Write	bot alias*		
DeleteSlot	Gewährt die Berechtigung zum Löschen eines vorhandenen Slots in einer Absicht	Write	bot*		
DeleteSlotType	Gewährt die Berechtigung zum Löschen eines vorhandenen Slot-Typs in einer Bot-Locale	Schreiben	bot*		
DeleteTestSet	Gewährt die Berechtigung, einen bestehenden Testsatz zu löschen	Schreiben	test set*		
DeleteUtterances	Gewährt die Berechtigung zum Löschen von Äußerungsdaten für einen Bot	Schreiben	bot*		
DescribeBot	Gewährt die Erlaubnis, einen bestehenden Bot abzurufen	Read	bot*		
DescribeBotAlias	Gewährt die Berechtigung zum Abrufen eines bestehenden Bot-Alias	Read	bot alias*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeBotChannel [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen eines bestehenden Bot-Channels	Read	bot*		
DescribeBotLocale	Gewährt die Berechtigung zum Abrufen eines vorhandenen Bot-Gebietsschemas	Lesen	bot*		
DescribeBotRecommendation	Gewährt die Berechtigung zum Abrufen von Metadaten zu einer Bot-Empfehlung	Lesen	bot*		
DescribeBotReplica	Gewährt die Berechtigung zum Abrufen eines vorhandenen Bot-Replikats	Lesen	bot*		
DescribeBotResourceGeneration	Gewährt die Berechtigung zum Abrufen von Metadaten für die Generierung von Bot-Ressourcen	Lesen	bot*		
DescribeBotVersion	Gewährt die Berechtigung zum Abrufen einer bestehenden Bot-Version	Lesen	bot*		
DescribeCustomVocabulary [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von bestehendem benutzerdefiniertem Vokabular	Lesen	bot*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeCustomVocabularyMetadata	Gewährt die Berechtigung zum Abrufen von Metadaten von bestehendem benutzerdefiniertem Vokabular	Lesen	bot*		
DescribeExport	Gewährt die Berechtigung zum Abrufen eines vorhandenen Exports	Read	bot		lex:DescribeBot lex:DescribeBotLocale lex:DescribeIntent lex:DescribeSlot lex:DescribeSlotType lex:ListBotLocales lex:ListIntents lex:ListSlotTypes lex:ListSlots

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			test set		
DescribeImport	Gewährt die Berechtigung zum Abrufen eines vorhandenen Imports	Read	bot		
			test set		
DescribeIntent	Gewährt die Berechtigung, eine bestehende Absicht abzurufen	Read	bot*		
DescribeResourcePolicy	Gewährt die Berechtigung zum Abrufen einer bestehenden Ressourcenrichtlinie für eine Lex-Ressource	Read	bot		
			bot alias		
DescribeSlot	Gewährt die Berechtigung zum Abrufen eines vorhandenen Slots	Read	bot*		
DescribeSlotType	Gewährt die Berechtigung zum Abrufen eines vorhandenen Slot-Typs	Lesen	bot*		
DescribeTestExecution	Gewährt die Berechtigung, Metadaten zur Testausführung abzurufen	Lesen	test set*		
DescribeTestSet	Gewährt die Berechtigung, einen bestehenden Testsatz abzurufen	Lesen	test set*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeTestSetDiscrepancyReport	Gewährt die Berechtigung, einen Bericht über Testsatzunstimmigkeiten abzurufen	Lesen	test set*		
DescribeTestSetGeneration	Gewährt die Berechtigung, Metadaten zur Testsatzgenerierung abzurufen	Lesen	test set		
GenerateBotElement	Gewährt die Berechtigung zum Generieren unterstützter Felder oder Elemente für einen Bot	Lesen	bot*		
GetSession	Gewährt die Berechtigung zum Abrufen von Sitzungsinformationen für einen Bot-Alias und eine Benutzer-ID	Lesen	bot alias*		
GetTestExecutionArtifactsUrl	Gewährt die Berechtigung, die Artefakt-URL für eine Testausführung abzurufen	Lesen	test set*		
ListAggregatedUtterances	Gewährt die Berechtigung zum Auflisten von Äußerungen und Statistiken für einen Bot	Auflisten	bot*		
ListBotAliasReplicas	Gewährt die Berechtigung zum Auflisten von Aliasreplikaten in einem Bot-Replikat	Auflisten	bot*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListBotAliases	Gewährt die Berechtigung, Bot-Aliase in einem Bot aufzulisten	List	bot*		
ListBotChannels [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Bot-Channels.	List	bot*		
ListBotLocales	Gewährt die Berechtigung zum Auflisten von Bot-Locales in einem Bot	Auflisten	bot*		
ListBotRecommendations	Gewährt die Berechtigung zum Abrufen einer Liste von Bot-Empfehlungen, die die angegebenen Kriterien erfüllen	Auflisten	bot*		
ListBotReplicas	Gewährt die Berechtigung zum Auflisten von Replikaten eines Bots	Auflisten	bot*		
ListBotResourceGenerations	Gewährt die Berechtigung zum Auflisten der Ressourcengenerierungen für einen Bot	Auflisten	bot*		
ListBotVersionReplicas	Gewährt die Berechtigung zum Auflisten von Versionsreplikaten in einem Bot-Replikat	Auflisten	bot*		
ListBotVersions	Gewährt die Berechtigung zum Auflisten bestehender Bot-Versionen	List	bot*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListBots	Gewährt die Berechtigung zum Auflisten vorhandener Ledger	List			
ListBuiltInIntents	Gewährt die Berechtigung zum Auflisten von integrierten Absichten	List			
ListBuiltInSlotTypes	Gewährt die Berechtigung zum Auflisten von integrierten Slot-Typen	Auflisten			
ListCustomVocabularyItems	Gewährt die Berechtigung zum Auflisten von Elementen in einem bestehendem benutzerdefiniertem Vokabular	Auflisten	bot*		
ListExports	Gewährt die Berechtigung zum Auflisten vorhandener Exporte	List			
ListImports	Gewährt die Berechtigung zum Auflisten vorhandener Importe	Auflisten			
ListIntentMetrics	Gewährt die Berechtigung, Intent-Analytics-Metriken für einen Bot aufzulisten	Auflisten	bot*		
ListIntentPaths	Gewährt die Berechtigung, Intent-Pfad-Analytics für einen Bot aufzulisten	Auflisten	bot*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListIntentStageMetrics	Gewährt die Berechtigung, intentStage-Analytics-Metriken für einen Bot aufzulisten	Auflisten	bot*		
ListIntents	Gewährt die Berechtigung, Absichten in einem Bot aufzulisten	Auflisten	bot*		
ListRecommendedIntents	Gewährt die Berechtigung, eine Liste der empfohlenen Absichten zu erhalten, die durch die Bot-Empfehlung bereitgestellt werden	Auflisten	bot*		
ListSessionAnalyticsData	Gewährt die Berechtigung, Sitzungs-Analytics-Daten für einen Bot aufzulisten	Auflisten	bot*		
ListSessionMetrics	Gewährt die Berechtigung, Sitzungs-Analytics-Metriken für einen Bot aufzulisten	Auflisten	bot*		
ListSlotTypes	Gewährt die Berechtigung zum Auflisten von Slot-Typen in einem Bot	List	bot*		
ListSlots	Gewährt die Erlaubnis, Slots in einer Absicht aufzulisten	List	bot*		
ListTagsForResource	Gewährt Erlaubnis, Tags für eine Lex Ressource zu listen	Lesen	bot		
			bot alias		
			test set		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTestExecutionResultItems	Gewährt die Berechtigung, Ergebnisdaten einer Testausführung abzurufen	Lesen	test set*		lex:ListTestSetRecords
ListTestExecutions	Gewährt die Berechtigung, Testausführungen aufzulisten	Auflisten			
ListTestSetRecords	Gewährt die Berechtigung, Datensätze aus einem bestehenden Testsatz abzurufen	Lesen	test set*		
ListTestSets	Gewährt die Berechtigung, Testsätze aufzulisten	Auflisten			
PutSession	Gewährt die Berechtigung zum Erstellen einer neuen Sitzung oder zum Ändern einer vorhandenen Sitzung für einen Bot-Alias und eine Benutzer-ID	Schreiben	bot alias*		
RecognizeText	Gewährt die Berechtigung zum Senden von Benutzereingaben (nur Text) an einen Bot-Alias	Schreiben	bot alias*		
RecognizeUtterance	Gewährt die Berechtigung zum Senden von Benutzereingaben (Text oder Sprache) an einen Bot-Alias	Schreiben	bot alias*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SearchAssociatedTranscripts	Gewährt die Berechtigung zum Suchen nach zugeordneten Transkripten, die die angegebenen Kriterien erfüllen	Auflisten	bot*		
StartBotRecommendation	Gewährt die Berechtigung zum Starten einer Bot-Empfehlung für ein vorhandenes Bot-Gebietsschema	Schreiben	bot*		
StartBotResourceGeneration	Gewährt die Berechtigung zum Starten einer Ressourcengenerierung für ein vorhandenes Bot-Gebietsschema	Schreiben	bot*		
StartConversation	Gewährt die Berechtigung zum Streamen von Benutzereingaben (Speech/Text/DTMF) an einen Bot-Alias	Write	bot alias*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartImport	Gewährt die Berechtigung zum Starten eines neuen Imports mit der hochgeladenen Importdatei	Schreiben	bot		lex:CreateBot lex:CreateBotLocale lex:CreateCustomVocabulary lex:CreateIntent lex:CreateSlot lex:CreateSlotType lex:CreateTestSet lex:DeleteBotLocale lex:DeleteCustomVocabulary lex:DeleteIntent

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					lex:DeleteSlot lex:DeleteSlotType lex:UpdateBot lex:UpdateBotLocale lex:UpdateCustomVocabulary lex:UpdateIntent lex:UpdateSlot lex:UpdateSlotType lex:UpdateTestSet
			bot alias		
			test set		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
StartTestExecution	Gewährt die Berechtigung, eine Testausführung mit einem Testsatz zu starten	Schreiben	test set*		
StartTestSetGeneration	Gewährt die Berechtigung, einen Testsatz zu generieren	Schreiben	test set		
StopBotRecommendation	Gewährt die Berechtigung zum Stoppen einer Bot-Empfehlung für ein vorhandenes Bot-Gebietsschema.	Schreiben	bot*		
TagResource	Gewährt die Berechtigung zum Hinzufügen oder Überschreiben von Tags einer Lex Ressource	Markieren	bot		
			bot alias		
			test set		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource		Markieren	bot		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Gewährt die Berechtigung zum Entfernen von Tags aus einer Lex-Ressource		bot alias		
			test set		
				aws:TagKeys	
UpdateBot	Gewährt die Erlaubnis, einen bestehenden Bot zu aktualisieren	Write	bot*		
UpdateBotAlias	Gewährt die Berechtigung, einen bestehenden Bot-Alias zu aktualisieren	Write	bot alias*		
UpdateBotLocale	Ermöglicht das Aktualisieren einer vorhandenen Bot-Locale	Schreiben	bot*		
UpdateBotRecommendation	Gewährt die Berechtigung zum Aktualisieren eines einer bestehenden Bot-Empfehlungs-Anforderung	Schreiben	bot*		
UpdateCustomVocabulary [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren von bestehendem benutzerdefiniertem Vokabular	Schreiben	bot*		
UpdateExport	Gewährt die Berechtigung zum Aktualisieren eines vorhandenen Exports	Write	bot*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateIntent	Gewährt die Erlaubnis, eine bestehende Absicht zu aktualisieren	Write	bot*		
UpdateResourcePolicy	Gewährt die Berechtigung zum Aktualisieren einer bestehenden Ressourcenrichtlinie für eine Lex-Ressource	Write	bot		
			bot alias		
UpdateSlot	Gewährt die Berechtigung zum Aktualisieren eines vorhandenen Slots	Write	bot*		
UpdateSlotType	Gewährt die Berechtigung zum Aktualisieren eines vorhandenen Slot-Typs	Schreiben	bot*		
UpdateTestSet	Gewährt die Berechtigung, einen bestehenden Testsatz zu aktualisieren	Schreiben	test set*		

Von Amazon Lex V2 definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
bot	`arn:${Partition}:lex:${Region}:${Account}:bot/${BotId}`	aws:ResourceTag/${TagKey}
bot alias	`arn:${Partition}:lex:${Region}:${Account}:bot-alias/${BotId}/${BotAliasId}`	aws:ResourceTag/${TagKey}
test set	`arn:${Partition}:lex:${Region}:${Account}:test-set/${TestSetId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Lex V2

Amazon Lex V2 definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den Tags in der Anforderung.	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff über die Tags, die einer Lex-Ressource zugeordnet sind.	String
aws:TagKeys	Filtert den Zugriff nach dem Satz von Tag-Schlüsseln in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS License Manager

AWS License Manager (Servicepräfix: `license-manager`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS License Manager definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptGrant	Gewährt die Berechtigung zum Annehmen einer Berechtigung	Write	grant*		
CheckInLicense	Gewährt die Berechtigung, Lizenzberechtigungen wieder in den Pool einzuchecken	Write			
CheckoutBorrowLicense	Gewährt die Berechtigung, Lizenzberechtigungen für Ausleih-Anwendungsfälle auszuchecken	Write	license*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CheckoutLicense	Gewährt die Berechtigung, Lizenzberechtigungen auszuchecken	Write			
CreateGrant	Gewährt die Berechtigung zum Erstellen einer neuen Berechtigung für eine Lizenz	Write	license*		
CreateGrantVersion	Gewährt die Berechtigung zum Erstellen einer neuen Version einer Berechtigung	Write	grant*		
CreateLicense	Gewährt die Berechtigung zum Erstellen einer neuen Lizenz	Write			
CreateLicenseConfiguration	Gewährt die Berechtigung zum Erstellen einer neuen Lizenzkonfiguration	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicenseConversionTaskForResource	Gewährt die Berechtigung zum Erstellen einer Lizenzkonvertierungsaufgabe für eine Ressource	Schreiben			
CreateLicenseManagerReportGenerator	Gewährt die Berechtigung zum Erstellen eines Berichtsgenerators für eine Lizenzkonfiguration	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateLicenseVersion	Gewährt die Berechtigung zum Erstellen einer neuen Version der Lizenz	Schreiben	license*		
CreateToken	Gewährt die Berechtigung zum Erstellen eines neuen Tokens für die Lizenz	Schreiben	license*		
DeleteGrant	Gewährt die Berechtigung zum Löschen einer Erteilung	Schreiben	grant*		
DeleteLicense	Gewährt die Berechtigung zum Löschen einer Lizenz	Write	license*		
DeleteLicenseConfiguration	Gewährt die Berechtigung zum dauerhaften Löschen einer Lizenzkonfiguration	Write	license-configuration*		
DeleteLicenseManagerReportGenerator	Gewährt die Berechtigung zum Löschen eines Berichtsgenerators	Write	report-generator*		
DeleteToken	Gewährt die Berechtigung zum Löschen eines Tokens	Write			
ExtendLicenseConsumption	Gewährt die Berechtigung zum Verlängern der Nutzungszeit für bereits ausgecheckte Lizenzberechtigungen	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAccessToken	Gewährt die Berechtigung zum Abrufen des Zugriffstokens	Read			
GetGrant	Gewährt die Berechtigung zum Abrufen einer Berechtigung	Read	grant*		
GetLicense	Gewährt die Berechtigung zum Abrufen einer Lizenz	Read	license*		
GetLicenseConfiguration	Gewährt die Berechtigung zum Abrufen einer Lizenzkonfiguration	Lesen	license-configuration*		
GetLicenseConversionTask	Gewährt die Berechtigung zum Abrufen einer Lizenzkonvertierungsaufgabe	Lesen			
GetLicenseManagerReportGenerator	Gewährt die Berechtigung zum Abrufen eines Berichtsgenerators	Read	report-generator*		
GetLicenseUsage	Gewährt die Berechtigung zum Abrufen einer Lizenznutzung	Read	license*		
GetServiceSettings	Gewährt die Berechtigung zum Abrufen von Serviceeinstellungen	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAssociationsForLicenseConfiguration	Gewährt die Berechtigung zum Auflisten von Mappings für eine ausgewählte Lizenzkonfiguration	List	license-configuration*		
ListDistributedGrants	Gewährt die Berechtigung zum Auflisten vGewährter Berechtigungen	List			
ListFailuresForLicenseConfigurationOperations	Gewährt die Berechtigung zum Auflisten der fehlgeschlagenen Lizenzkonfigurationsvorgänge	List	license-configuration*		
ListLicenseConfigurations	Gewährt die Berechtigung zum Auflisten von Lizenzkonfigurationen	Lesen			
ListLicenseConversionTasks	Gewährt die Berechtigung zum Auflisten von Lizenzkonvertierungsaufgaben	Auflisten			
ListLicenseManagerReportGenerators	Gewährt die Berechtigung zum Auflisten von Berichtsgeneratoren	List	license-configuration		
ListLicenseSpecificationsForResource	Gewährt die Berechtigung zum Auflisten der Lizenzspezifikationen, die einer ausgewählten Ressource zugeordnet sind	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListLicenseVersions	Gewährt die Berechtigung zum Auflisten von Lizenzversionen	List	license*		
ListLicenses	Gewährt die Berechtigung zum Auflisten von Lizenzen	Lesen			
ListReceivedGrants	Gewährt die Berechtigung zum Auflisten erhaltener Berechtigungen	Auflisten			
ListReceivedGrantsForOrganization	Gewährt die Berechtigung zum Auflisten erhaltener Berechtigungen	Auflisten			
ListReceivedLicenses	Gewährt die Berechtigung zum Auflisten erhaltener Lizenzen	Auflisten			
ListReceivedLicensesForOrganization	Gewährt die Berechtigung zum Auflisten erhaltener Lizenzen für die Organisation	Auflisten			
ListResourceInventory	Gewährt die Berechtigung zum Auflisten von Ressourcenbestand	List			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine ausgewählte Ressource	Lesen	license-configuration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTokens	Gewährt die Berechtigung zum Auflisten von Tokens	List			
ListUsageForLicenseConfiguration	Gewährt die Berechtigung zum Auflisten von Nutzungsdatensätzen für eine ausgewählte Lizenzkonfiguration	List	license-configuration*		
RejectGrant	Gewährt die Berechtigung zum Ablehnen einer Berechtigung	Write	grant*		
TagResource	Gewährt die Berechtigung zum Markieren einer ausgewählten Ressource	Markieren	license-configuration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer ausgewählten Ressource	Markieren	license-configuration*		
UpdateLicenseConfiguration	Gewährt die Berechtigung zum Aktualisieren einer bestehenden Lizenzkonfiguration	Write	license-configuration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateLicenseManagerReportGenerator	Gewährt die Berechtigung zum Aktualisieren eines Berichtsgenerators für eine Lizenzkonfiguration	Write	report-generator*		
UpdateLicenseSpecificationsForResource	Gewährt die Berechtigung zum Aktualisieren von Lizenzspezifikationen für eine ausgewählte Ressource	Write	license-configuration*		
UpdateServiceSettings	Gewährt die Berechtigung zum Aktualisieren von Serviceeinstellungen	Berechtigungsverwaltung			

Von AWS License Manager definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
license-configuration	`arn:${Partition}:license-manager:${Region}:${Account}:license-configuration:${LicenseConfigurationId}`	license-manager:ResourceTag/${TagKey}
license	`arn:${Partition}:license-manager::${Account}:license:${LicenseId}`	

Ressourcentypen	ARN	Bedingungsschlüssel
grant	`arn:${Partition}:license-manager::${Account}:grant:${GrantId}`	
report-generator	`arn:${Partition}:license-manager:${Region}:${Account}:report-generator:${ReportGeneratorId}`	license-manager:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS License Manager

AWS License Manager definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf Tag-Schlüsseln, die in der Anforderung übergeben werden	ArrayOfString
license-manager:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüsselwertpaaren, die der Ressource angefügt sind	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für AWS License Manager Linux Subscriptions Manager

AWS License Manager Linux Subscriptions Manager (Servicepräfix: `license-manager-linux-subscriptions`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS License Manager Linux Subscriptions Manager definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetServiceSettings	Gewährt die Berechtigung zum Abrufen der Service-Einstellungen für Linux-Abonnements in AWS License Manager	Lesen			
ListLinuxSubscriptionInstances	Gewährt die Berechtigung zum Auflisten aller Instances mit Linux-Abonnements in AWS License Manager	Lesen			
ListLinuxSubscriptions	Gewährt die Berechtigung zum Auflisten aller Linux-Abo	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	nnements in AWS License Manager				
UpdateServiceSettings	Gewährt die Berechtigung zum Aktualisieren der Service-Einstellungen für Linux-Abonnements in AWS License Manager	Schreiben			

Von AWS License Manager Linux Subscriptions Manager definierte Ressourcentypen

AWS License Manager Linux Subscriptions Manager unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um Zugriff auf AWS License Manager Linux Subscriptions Manager zu erteilen, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS License Manager Linux Subscriptions Manager

License Manager Linux Subscriptions Manager besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS License Manager User Subscriptions

AWS License Manager User Subscriptions (Servicepräfix: `license-manager-user-subscriptions`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.

- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS License Manager User Subscriptions definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateUser	Gewährt die Berechtigung, einen abonnierten Benutzer mit einer Instance zu verknüpfen, die mit License Manager User Subscriptions-Produkten gestartet wurde	Schreiben			
DeregisterIdentityProvider	Gewährt die Berechtigung, die Registrierung von Microsoft Active Directory mit License-Manager-User-Subscriptions für ein Produkt aufzuheben	Schreiben			
DisassociateUser	Gewährt die Berechtigung, einen abonnierten Benutzer von einer Instance zu trennen, die mit License Manager User Subscriptions-Produkten gestartet wurde	Schreiben			
ListIdentityProviders	Gewährt die Berechtigung zum Auflisten aller Identität	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	sanbieter für License Manager User Subscriptions				
ListInstances	Gewährt die Berechtigung zum Auflisten aller Instances, die mit License Manager User Subscriptions-Produkten gestartet wurden	Auflisten			
ListProductSubscriptions	Gewährt die Berechtigung zum Auflisten aller Produktabonnements für ein Produkt und einen Identitätsanbieter	Auflisten			
ListUserAssociations	Gewährt die Berechtigung, alle Benutzer aufzulisten, die einer für ein Produkt gestarteten Instance zugeordnet sind	Auflisten			
RegisterIdentityProvider	Gewährt die Berechtigung zum Registrieren von Microsoft Active Directory mit License-Manager-User-Subscriptions für ein Produkt	Schreiben			
StartProductSubscription	Gewährt die Berechtigung zum Starten eines Produktabonnements für einen Benutzer in einem registrierten aktiven Verzeichnis für ein Produkt	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopProductSubscription	Gewährt die Berechtigung zum Beenden des Produktabonnements für einen Benutzer in einem registrierten Active Directory für ein Produkt	Schreiben			
UpdateIdentityProviderSettings	Gewährt die Berechtigung zum Aktualisieren der Konfiguration des Identitätsanbieters	Schreiben			

Von AWS License Manager User Subscriptions definierte Ressourcentypen

AWS License Manager User Subscriptions unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um Zugriff auf AWS License Manager User Subscriptions zu erteilen, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS License Manager User Subscriptions

License Manager User Subscriptions besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Lightsail

Amazon Lightsail (Servicepräfix: `lightsail`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.

- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Lightsail definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AllocateStaticIp	Erstellt eine statische IP-Adresse, die an eine Instance angefügt werden kann.	Write			
AttachCertificateToDistribution	Gewährt die Berechtigung zum Anhängen eines SSL/TLS-Zertifikats an Ihre Amazon Lightsail Content Delivery Network (CDN)-Distribution	Write	Certificate*		
			Distribution*		
AttachDisk	Gewährt die Berechtigung zum Zuordnen eines Datenträgers an eine Instance	Write	Disk*		
AttachInstancesToLoadBalancer	Gewährt Berechtigungen eine oder mehrere Instances an einen Load Balancer anzuhängen	Write	LoadBalancer*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AttachLoadBalancerTlsCertificate	Gewährt Berechtigungen ein TLS-Zertifikat an einen Load Balancer anzuhängen	Write	LoadBalancer*		
AttachStaticIp	Gewährt die Berechtigung zum Anhängen einer statischen IP-Adresse an eine Instance	Write	Instance*		
			StaticIp*		
CloseInstancePublicPorts	Gewährt die Berechtigung zum Schließen eines öffentlichen Ports einer Instance	Schreiben	Instance*		
CopySnapshot	Gewährt die Berechtigung zum Kopieren eines Snapshots von einem AWS-Region in ein anderes in Amazon Lightsail	Schreiben			
CreateBucket	Gewährt die Berechtigung zum Erstellen eines Amazon Lightsail-Buckets	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateBucketAccessKey	Gewährt die Berechtigung zum Erstellen eines Zugriffsschlüssels für den angegebenen Bucket	Write	Bucket*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCertificate	Gewährt die Berechtigung zum Erstellen eines SSL/TLS-Zertifikats	Write		aws:RequestTag/${TagKey} aws:TagKeys	lightsail:CreateDomainEntry lightsail:GetDomains
CreateCloudFormationStack	Gewährt die Berechtigung zur Erstellung einer neuen Amazon EC2-Instance aus einem exportierten Amazon Lightsail-Snapshot	Write			
CreateContactMethod	Gewährt die Berechtigung zum Erstellen einer Kontaktmethode für E-Mail- oder SMS-Nachrichten	Write			
CreateContainerService	Gewährt die Berechtigung zum Erstellen eines Amazon Lightsail-Container-Services	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateContainerServiceDeployment	Gewährt die Berechtigung zum Erstellen einer Bereitstellung für Ihren Amazon Lightsail-Container-Services	Write	ContainerService*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateContainerServiceRegistryLogin	Gewährt die Berechtigung zum Erstellen eines temporären Anmeldeinformationssatzes, mit dem Sie sich beim Docker-Prozess auf Ihrem lokalen Computer anmelden können	Write			
CreateDisk	Gewährt die Berechtigung zum Erstellen eines Datenträgers.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDiskFromSnapshot	Gewährt die Berechtigung zum Erstellen eines Datenträgers für Snapshot	Write	DiskSnapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDiskSnapshot	Gewährt die Berechtigung zum Erstellen eines neuen Snapshot-Datenträgers	Write	Disk		
			Instance		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDistribution	Gewährt die Berechtigung zum Erstellen einer Amazon Lightsail Content Delivery Network (CDN)-Distribution	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDomain	Gewährt die Berechtigung zum Erstellen einer Domain-Ressource für den angegebenen Domain-Namen	Write		aws:RequestTag/${TagKey} aws:TagKeys	route53:DeleteHostedZone route53:GetHostedZone route53:ListHostedZonesByName route53domains:GetDomainDetail route53domains:GetOperationDetail route53domains:ListDomains route53domains:ListOperations route53domains:Upd

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ateDomainNameservers
CreateDomainEntry	Gewährt die Berechtigung einen oder mehrere DNS-Datensatzeinträge für eine Domain-Ressource zu erstellen: Adresse (A), kanonischer Name (CNAME), Mail Exchanger (MX), Nameserver (NS), Start of Authority (SOA), Service Locator (SRV) oder Text (TXT)	Schreiben	Domain*		
CreateGUISessionAccessDetails	Gewährt die Berechtigung zum Erstellen von URLs, die für den Zugriff auf die GUI (grafische Benutzeroberfläche)-Sitzung einer Instance verwendet werden	Schreiben	Instance*		
CreateInstanceSnapshot	Gewährt die Berechtigung zum Erstellen einer Snapshot-Instance	Write	Instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateInstances	Gewährt die Berechtigung zum Erstellen einer oder mehrerer Instances	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateInstancesFromSnapshot	Gewährt die Berechtigung eine oder mehrere Instances basierend auf einem Instance-Snapshot zu erstellen	Write	InstanceSnapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateKeyPair	Gewährt die Berechtigung, ein Schlüsselpaar für die Authentifizierung und die Verbindung mit einer Instance zu erstellen	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLoadBalancer	Gewährt die Berechtigung zum Erstellen eines Load Balancers	Write		aws:RequestTag/${TagKey} aws:TagKeys	lightsail:CreateDomainEntry lightsail:GetDomains

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateLoadBalancerTlsCertificate	Gewährt die Berechtigung zum Erstellen einer Lastenverteilung/TLS-Zertifikats	Write	LoadBalancer*		lightsail:CreateDomainEntry lightsail:GetDomains
CreateRelationalDatabase	Gewährt die Berechtigung zum Erstellen einer neuen relationalen Datenbank	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRelationalDatabaseFromSnapshot	Gewährt die Berechtigung eine neue relationale Datenbank aus einem Snapshot zu erstellen	Write	RelationalDatabaseSnapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRelationalDatabaseSnapshot	Gewährt die Berechtigung zum Erstellen eines relationalen Datenbank-Snapshots	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteAlarm	Gewährt die Berechtigung zum Löschen eines Alarms	Write	Alarm*		
DeleteAutoSnapshot	Gewährt die Berechtigung zum Löschen eines automatischen Snapshots einer Instance oder eines Datenträgers	Write			
DeleteBucket	Gewährt die Berechtigung zum Löschen eines Amazon-Lightsail-Buckets	Write	Bucket*		
DeleteBucketAccessKey	Gewährt die Berechtigung zum Löschen eines Zugriffsschlüssels für den angegebenen Amazon-Lightsail-Bucket	Write	Bucket*		
DeleteCertificate	Gewährt die Berechtigung zum Löschen eines SSL/TLS-Zertifikats	Write	Certificate*		
DeleteContactMethod	Gewährt die Berechtigung zum Löschen einer Kontaktmethode	Write			
DeleteContainerImage	Gewährt die Berechtigung zum Löschen eines Container-Images, das bei Ihrem Amazon Lightsail-Container-Service registriert ist	Write	ContainerService*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteContainerService	Gewährt die Berechtigung zum Löschen Ihres Amazon Lightsail-Container-Services	Write	ContainerService*		
DeleteDisk	Gewährt die Berechtigung zum Löschen eines Datenträgers	Write	Disk*		
DeleteDiskSnapshot	Gewährt die Berechtigung zum Löschen eines Snapshot-Datenträgers	Write	DiskSnapshot*		
DeleteDistribution	Gewährt die Berechtigung zum Löschen Ihrer Amazon Lightsail Content Delivery Network (CDN)-Distribution	Write	Distribution*		
DeleteDomain	Gewährt die Berechtigung zum Löschen eine Domain-Ressource und aller zugehörigen DNS-Datensätze	Write	Domain*		
DeleteDomainEntry	Gewährt die Berechtigung zum Löschen eines DNS-Eintrag für eine Domain-Ressource	Write	Domain*		
DeleteInstance	Gewährt die Berechtigung zum Löschen einer Instance	Write	Instance*		
DeleteInstanceSnapshot	Gewährt die Berechtigung zum Löschen eines Instance-Snapshots	Write	InstanceSnapshot*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteKeyPair	Gewährt die Berechtigung zum Löschen eines Schlüsselpaares, das für die Authentifizierung und die Verbindung mit einer Instance verwendet wird	Write	KeyPair*		
DeleteKnownHostKeys	Gewährt die Berechtigung zum Löschen des bekannten Host-Schlüssel oder das von Browser-basierten SSH- oder RDP-Clients von Amazon Lightsail zur Authentifizierung einer Instance verwendete Zertifikat	Write	Instance*		
DeleteLoadBalancer	Gewährt die Berechtigung zum Löschen eines Load Balancer	Write	LoadBalancer*		
DeleteLoadBalancerTlsCertificate	Gewährt die Berechtigung zum Löschen eines Load Balancer TLS-Zertifikats	Write	LoadBalancer*		
DeleteRelationalDatabase	Gewährt die Berechtigung zum Löschen einer relationalen Datenbank.	Write	RelationalDatabase*		
DeleteRelationalDatabaseSnapshot	Gewährt die Berechtigung zum Löschen eines relationalen Datenbank-Snapshots	Write	RelationalDatabaseSnapshot*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DetachCertificateFromDistribution	Gewährt die Berechtigung zum Trennen eines SSL/TLS-Zertifikats von Ihrer Amazon Lightsail Content Delivery Network (CDN)-Distribution	Write	Distribution*		
DetachDisk	Gewährt die Berechtigung zum Trennen eines Datenträgers von einer Instance	Write	Disk*		
DetachInstancesFromLoadBalancer	Gewährt die Berechtigung zum Trennen eines oder mehrerer Instances von einem -Load-Balancer	Write	LoadBalancer*		
DetachStaticIp	Gewährt die Berechtigung zum Trennen einer statische IP von einer Instance, an die sie angefügt ist	Write	StaticIp*		
DisableAddOn	Gewährt die Berechtigung zum Deaktivieren eines Add-ons für eine Amazon Lightsail-Ressource	Schreiben			
DownloadDefaultKeyPair	Gewährt die Berechtigung zum Herunterladen des Standard-Schlüsselpaars, das für die Authentifizierung und Verbindung mit Instances in einer bestimmten verwendet wird AWS-Region	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
EnableAddOn	Gewährt die Berechtigung zum Aktivieren oder Ändern eines Add-ons für eine Amazon Lightsail-Ressource	Write			
ExportSnapshot	Gewährt die Berechtigung einen Amazon-Lightsail-Snapshot nach Amazon EC2 zu exportieren	Write	DiskSnapshot		iam:CreateServiceLinkedRole iam:PutRolePolicy
			InstanceSnapshot		
GetActiveNames	Gewährt die Berechtigung zum Abrufen der Namen aller aktiven (nicht gelöschten) Ressourcen	Read			
GetAlarms	Gewährt die Berechtigung zum Anzeigen von Informationen über die konfigurierten Alarme	Read			
GetAutoSnapshots	Gewährt die Berechtigung zum Anzeigen der verfügbaren automatischen Snapshots für eine Instance oder einen Datenträger	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBlueprints	Gewährt die Berechtigung zum Abrufen einer Liste von Instance-Abbildern oder -Vorlagen Sie können eine Vorlage zum Erstellen einer neuen Instance verwenden, die bereits ein bestimmtes Betriebssystem ausführt, aber auch eine vorinstallierte App oder einen Entwicklungs-Stack. Die Software, die auf Ihrer Instance ausgeführt wird, hängt von der Vorlage ab, die Sie beim Erstellen der Instance definieren.	Read			
GetBucketAccessKeys	Gewährt die Berechtigung zum Abrufen der vorhandenen Zugriffsschlüssel-IDs für den angegebenen Amazon-Lightsail-Bucket	Read			
GetBucketBundles	Gewährt die Berechtigung zum Abrufen der Bundles, die auf einen Amazon Lightsail -Bucket angewendet werden können	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBucketMetricData	Gewährt die Berechtigung zum Abrufen der Datenpunkte einer bestimmten Metrik für einen Amazon Lightsail -Bucket	Read			
GetBuckets	Gewährt die Berechtigung zum Anzeigen von Informationen über ein oder mehrere Amazon Lightsail-Buckets	Read			
GetBundles	Gewährt die Berechtigung zum Abrufen einer Liste von Instance-Bundles Sie können ein Paket verwenden, um eine neue Instance mit einer Reihe von Leistungsspezifikationen wie CPU-Anzahl, Festplattengröße, RAM-Größe und Netzwerkübertragungskontingent zu erstellen. Die Kosten Ihrer Instance hängen vom Paket ab, das Sie beim Erstellen der Instance definieren.	Read			
GetCertificates	Gewährt die Berechtigung zum Anzeigen von Informationen über ein oder mehrere Amazon Lightsail-SSL/TLS-Zertifikate	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetCloudFormationStackRecords	Gewährt die Berechtigung zum Abrufen von Informationen zu allen CloudFormation Stacks, die zum Erstellen von Amazon EC2-Ressourcen aus exportierten Amazon Lightsail-Snapshots verwendet werden	Lesen			
GetContactMethods	Gewährt die Berechtigung zum Anzeigen von Informationen über die konfigurierten Kontaktmethoden	Read			
GetContainerAPIMetadata	Gewährt die Berechtigung zum Anzeigen von Informationen über Amazon Lightsail-Container, wie die aktuelle Version des Lightsail-Control-Plugins (lightsailctl)	Read			
GetContainerImages	Gewährt die Berechtigung zum Anzeigen der Container-Images, die bei Ihrem Amazon Lightsail-Container-Service registriert sind	Read			
GetContainerLog	Gewährt die Berechtigung zum Anzeigen der Protokollereignisse eines Containers Ihres Amazon Lightsail-Container-Services	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetContainerServiceDeployments	Gewährt die Berechtigung zum Anzeigen der Bereitstellungen für Ihren Amazon Lightsail-Container-Service	Read			
GetContainerServiceMetricData	Gewährt die Berechtigung zum Anzeigen der Datenpunkte einer bestimmten Metrik Ihres Amazon Lightsail-Container-Service	Read			
GetContainerServicePowers	Gewährt die Berechtigung zum Anzeigen der Liste der Befugnisse, die für Ihre Amazon Lightsail-Containerservices angegeben werden können	Read			
GetContainerServices	Gewährt die Berechtigung zum Anzeigen von Informationen über einen oder mehrere Ihrer Amazon Lightsail-Container-Services	Lesen			
GetCostEstimate	Gewährt die Berechtigung zum Abrufen der Informationen zur Kostenschätzung für eine angegebene Ressource	Lesen	Disk Instance		
GetDisk	Gewährt Berechtigungen zum Abrufen von Informationen zu einem Datenträger.	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDiskSnapshot	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Festplattensnapshot	Read			
GetDiskSnapshots	Gewährt die Berechtigung zum Abrufen von Informationen zu allen Festplatten-Snapshots	Read			
GetDisks	Gewährt die Berechtigung zum Abrufen von Informationen zu allen Datenträgern	Read			
GetDistributionBundles	Gewährt die Berechtigung zum Anzeigen der Liste der Bundles, die auf Ihre Amazon Lightsail Content Delivery Network (CDN)-Distributionen angewendet werden können	Read			
GetDistributionLatestCacheReset	Gewährt die Berechtigung zum Anzeigen des Zeitstempels und des Status der letzten Cache-Zurücksetzung einer bestimmten Amazon Lightsail Content Delivery Network (CDN)-Distribution	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDistributionMetricData	Gewährt die Berechtigung zum Anzeigen der Datenpunkte einer bestimmten Metrik für eine Amazon Lightsail Content Delivery Network (CDN)-Distribution	Read			
GetDistributions	Gewährt die Berechtigung zum Anzeigen von Informationen über eine oder mehrere Ihrer Amazon Lightsail Content Delivery Network (CDN)-Distributionen	Read			
GetDomain	Gewährt die Berechtigung zum Abrufen von DNS-Datensätzen für eine Domainressource	Read			
GetDomains	Gewährt die Berechtigung, DNS-Datensätze für alle Domain-Ressourcen zu erhalten	Read			
GetExportSnapshotRecords	Gewährt die Berechtigung Informationen zu allen Datensätzen zurückzubekommen, um Amazon Lightsail-Snapshots nach Amazon EC2 zu exportieren	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetInstance	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Instance	Read			
GetInstanceAccessDetails	Gewährt die Berechtigung um temporäre Schlüssel zu bekommen, mit denen Sie sich bei einer Instance authentifizieren und sich mit ihr verbinden können	Write	Instance*		
GetInstanceMetricData	Gewährt die Berechtigung zum Abrufen der Datenpunkte für die angegebene Metrik einer Instance	Read			
GetInstancePortStates	Gewährt die Berechtigung zum Abrufen des Portstatus von einer Instance	Read			
GetInstanceSnapshot	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Snapshot-Instance	Read			
GetInstanceSnapshots	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Snapshot-Instance	Read			
GetInstanceState	Gewährt die Berechtigung zum Abrufen des Status von einer Instance	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetInstances	Gewährt die Berechtigung zum Abrufen von Informationen über alle Instances	Read			
GetKeyPair	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Schlüsselpaar	Read			
GetKeyPairs	Gewährt die Berechtigung zum Abrufen von Informationen zu allen Schlüsselpaaren	Lesen			
GetLoadBalancer	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Load Balancer	Lesen			
GetLoadBalancerMetricData	Gewährt die Berechtigung zum Bekommen von Datenpunkten für die angegebene Metrik eines Load Balancer	Read			
GetLoadBalancerTlsCertificates	Gewährt die Berechtigung zum Abrufen von Informationen zu den TLS-Zertifikaten eines Load Balancer	Lesen			
GetLoadBalancerTlsPolicies	Gewährt die Berechtigung zum Abrufen einer Liste der TLS-Sicherheitsrichtlinien, die Sie auf Lightsail Load Balancer anwenden können	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetLoadBalancers	Gewährt die Berechtigung zum Abrufen von Informationen zu Lastausgleichssystemen	Read			
GetOperation	Gewährt die Berechtigung zum Abrufen von Informationen zu einer bestimmten Produktion Produktionen umfassen Ereignisse wie das Erstellen einer Instance, das Zuordnen einer statischen IP-Adresse, das Anfügen einer statischen IP-Adresse usw.	Read			
GetOperations	Gewährt die Berechtigung zum Abrufen von Informationen zu einer bestimmten Produktion Produktionen umfassen Ereignisse wie das Erstellen einer Instance, das Zuordnen einer statischen IP-Adresse, das Anfügen einer statischen IP-Adresse usw.	Read			
GetOperationsForResource	Gewährt die Berechtigung zum Abrufen von Operationen für eine Ressource	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetRegions	Gewährt die Berechtigung zum Abrufen einer Liste aller gültigen AWS-Regionen für Amazon Lightsail	Lesen			
GetRelationalDatabase	Gewährt die Berechtigung zum Abrufen von Informationen zu einer relationalen Datenbank	Read			
GetRelationalDatabaseBlueprints	Gewährt die Berechtigung zum Abrufen einer Liste von Abbildern oder Vorlagen einer relationalen Datenbank Sie können eine Vorlage verwenden, um eine neue Datenbank zu erstellen, auf der eine bestimmte Datenbank-Engine ausgeführt wird. Die Datenbank-Engine, die auf Ihrer Datenbank ausgeführt wird, hängt von der Vorlage ab, die Sie beim Erstellen der relationalen Datenbank definieren.	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetRelationalDatabaseBundles	Gewährt die Berechtigung zum Abrufen einer Liste von relationalen Datenbankpaketen. Sie können ein Paket verwenden, um eine neue Datenbank mit einer Reihe von Leistungsspezifikationen wie CPU-Anzahl, Festplattengröße, RAM-Größe, Netzwerkübertragungskontingent und dem Standard einer hohen Verfügbarkeit zu erstellen. Die Kosten Ihrer Datenbank hängen vom Paket ab, das Sie beim Erstellen der relationalen Datenbank definieren.	Read			
GetRelationalDatabaseEvents	Gewährt die Berechtigung zum Abrufen von Ereignissen für eine relationale Datenbank	Read			
GetRelationalDatabaseLogEvents	Gewährt die Berechtigung zum Abrufen von Ereignissen für den angegebenen Protokollstream einer relationalen Datenbank	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetRelationalDatabaseLogStreams	Gewährt die Berechtigung zum Abrufen von Protokollstreams zurück, die für eine relationale Datenbank verfügbar sind	Read			
GetRelationalDatabaseMasterUserPassword	Gewährt die Berechtigung zum Abrufen des Master-Benutzerpassworts einer relationalen Datenbank	Write	RelationalDatabase*		
GetRelationalDatabaseMetricData	Gewährt die Berechtigung zum Abrufen der Datenpunkte für die angegebene Metrik einer relationalen Datenbank	Read			
GetRelationalDatabaseParameters	Gewährt die Berechtigung zum Abrufen der Parameter einer relationalen Datenbank	Read			
GetRelationalDatabaseSnapshot	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Snapshot einer relationalen Datenbank	Read			
GetRelationalDatabaseSnapshots	Gewährt die Berechtigung zum Abrufen von Informationen zu allen Snapshots einer relationalen Datenbank	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetRelationalDatabases	Gewährt die Berechtigung zum Abrufen von Informationen zu allen relationalen Datenbanken	Lesen			
GetSetupHistory	Gewährt die Berechtigung zum Abrufen detaillierter Informationen zu Einrichtungsanforderungen, die auf der angegebenen Ressource ausgeführt wurden	Lesen	Instance		
GetStaticIp	Gewährt die Berechtigung zum Abrufen von Informationen zu einer statistischen Pipeline.	Read			
GetStaticIps	Gewährt die Berechtigung, Informationen zu statische IP-Adressen zu erhalten	Read			
ImportKeyPair	Gewährt die Berechtigung zum Importieren eines öffentlichen Schlüssels aus einem Schlüsselpaar	Write			
IsVpcPeered	Gewährt die Berechtigung einen booleschen Wert zurückzugeben, der angibt, ob die Amazon Lightsail Virtual Private Cloud (VPC) per Peering verbunden ist	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
OpenInstancePublicPorts	Gewährt die Berechtigung zum Hinzufügen oder Öffnen eines öffentlichen Ports einer Instance.	Write	Instance*		
PeerVpc	Gewährt die Berechtigung zum Versuch die Amazon Lightsail Virtual Private Cloud (VPC) mit der Standard-VPC zu verbinden	Write			
PutAlarm	Gewährt die Berechtigung zum Erstellen oder Aktualisieren eines Alarms und verknüpft ihn mit der angegebenen Metrik	Write	Alarm*		
PutInstancePublicPorts	Gewährt die Berechtigung die angegebenen offenen Ports für eine Instance festzulegen und schließt alle Ports für jedes Protokoll, das nicht in der Anforderung enthalten ist	Write	Instance*		
RebootInstance	Gewährt die Berechtigung eine Instance neuzustarten, die sich im aktiven Zustand befindet	Write	Instance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RebootRelationalDatabase	Gewährt die Berechtigung eine relationale Datenbank neuzustarten, die sich in einem aktiven Zustand befindet	Write	RelationalDatabase*		
RegisterContainerImage	Gewährt die Berechtigung zum Registrieren eines Container-Image für Ihren Amazon Lightsail-Container-Service	Write	ContainerService*		
ReleaseStaticIp	Gewährt die Berechtigung zum Löschen einer statischen IP-Adresse	Write	StaticIp*		
ResetDistributionCache	Gewährt die Berechtigung zum Löschen der aktuell zwischengespeicherten Inhalte aus Ihrer Amazon Lightsail Content Delivery Network (CDN)-Distribution	Write	Distribution*		
SendContactMethodVerification	Gewährt die Berechtigung zum Senden einer Verifizierungsanfrage an eine E-Mail-Kontaktmethode, um sicherzustellen, dass sie dem Anforderer gehört	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SetIpAddressType	Gewährt die Berechtigung zum Festlegen des IP-Adresstyps für eine Amazon Lightsail -Ressource	Write	Distribution		
			Instance		
			LoadBalancer		
SetResourceAccessForBucket	Gewährt die Berechtigung zum Festlegen der Amazon Lightsail -Ressourcen, die auf den angegebenen Amazon Lightsail-Bucket zugreifen können	Schreiben	Bucket*		
			Instance*		
SetupInstanceHttps	Gewährt die Berechtigung zum Erstellen eines SSL-/TLS-Zertifikats und zum Installieren dieses Zertifikats auf einer angegebenen Instance	Schreiben	Instance*		lightsail:GetInstanceAccessDetails
StartGUISession	Gewährt die Berechtigung zum Initiieren einer GUI (grafische Benutzeroberfläche)-Sitzung, die für den Zugriff auf das Betriebssystem oder die Anwendung einer Instance verwendet wird	Schreiben	Instance*		
StartInstance	Gewährt die Berechtigung zum Starten einer Instance, die angehalten wurde	Write	Instance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartRelationalDatabase	Gewährt die Berechtigung zum Starten einer relationalen Datenbank, die sich in einem angehaltenen Zustand befindet	Schreiben	RelationalDatabase*		
StopGUISession	Gewährt die Berechtigung zum Beenden einer GUI (grafische Benutzeroberfläche)-Sitzung, die für den Zugriff auf das Betriebssystem oder die Anwendung einer Instance verwendet wird	Schreiben	Instance*		
StopInstance	Gewährt die Berechtigung zum Stoppen einer Instance	Write	Instance*		
StopRelationalDatabase	Gewährt die Berechtigung zum Stoppen einer relationalen Datenbank, die sich im Ausführungsstatus befindet	Write	RelationalDatabase*		
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren	Bucket		
			Certificate		
			ContainerService		
			Disk		
			DiskSnapshot		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			Distribution		
			Domain		
			Instance		
			InstanceSnapshot		
			KeyPair		
			LoadBalancer		
			RelationalDatabase		
			RelationalDatabaseSnapshot		
			StaticIp		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TestAlarm	Gewährt die Berechtigung zum Testen eines Alarms, indem ein Banner auf der Amazon Lightsail-Konsole angezeigt wird, oder wenn ein Benachrichtigungsauslöser für den angegebenen Alarm konfiguriert ist, indem eine Benachrichtigung an das Benachrichtigungsprotokoll gesendet wird	Write	Alarm*		
UnpeerVpc	Gewährt die Berechtigung zum Versuch, die Peering-Verbindung der Amazon Lightsail Virtual Private Cloud (VPC) zur Standard-VPC zu trennen	Write			
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Markieren	Bucket		
			Certificate		
			ContainerService		
			Disk		
			DiskSnapshot		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			Distribution		
			Domain		
			Instance		
			InstanceSnapshot		
			KeyPair		
			LoadBalancer		
			RelationalDatabase		
			RelationalDatabaseSnapshot		
			StaticIp		
				aws:TagKeys	
UpdateBucket	Gewährt die Berechtigung zum Aktualisieren eines bestehenden Amazon Lightsail-Buckets	Write	Bucket*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateBucketBundle	Gewährt die Berechtigung zum Aktualisieren des Pakets oder Speicherplans eines vorhandenen Amazon Lightsail -Buckets	Write	Bucket*		
UpdateContainerService	Gewährt die Berechtigung zum Aktualisieren der Konfiguration Ihres Amazon Lightsail-Container-Services, z. B. seine Leistungsfähigkeit, Skalierung und öffentliche Domain-Namen	Write	ContainerService*		
UpdateDistribution	Gewährt die Berechtigung zum Aktualisieren einer bestehenden Amazon Lightsail Content Delivery Network (CDN)-Distribution oder ihrer Konfiguration	Write	Distribution*		
UpdateDistributionBundle	Gewährt die Berechtigung zum Aktualisieren des Pakets Ihrer Amazon Lightsail Content Delivery Network (CDN)-Distribution	Write	Distribution*		
UpdateDomainEntry	Gewährt die Berechtigung zum Aktualisieren einer Domain-Datensatzmenge nach der Erstellung	Schreiben	Domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateInstanceMetadataOptions	Erteilt die Berechtigung zum Aktualisieren der Metadatenoptionen für eine Instance	Schreiben	Instance*		
UpdateLoadBalancerAttribute	Gewährt die Berechtigung zum Aktualisieren eines Load Balancer-Attribut, z. B. den Zustandsprüfungspfad und das Session-Sticking	Write	LoadBalancer*		
UpdateRelationalDatabase	Gewährt die Berechtigung zum Aktualisieren einer relationalen Datenbank.	Write	RelationalDatabase*		
UpdateRelationalDatabaseParameters	Gewährt die Berechtigung zum Aktualisieren der Parameter einer relationalen Datenbank	Write	RelationalDatabase*		

Von Amazon Lightsail definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Domain	arn:${Partition}:lightsail:${Region}:${Account}:Domain/${Id}	aws:ResourceTag/${TagKey}
Instance	arn:${Partition}:lightsail:${Region}:${Account}:Instance/${Id}	aws:ResourceTag/${TagKey}
InstanceSnapshot	arn:${Partition}:lightsail:${Region}:${Account}:InstanceSnapshot/${Id}	aws:ResourceTag/${TagKey}
KeyPair	arn:${Partition}:lightsail:${Region}:${Account}:KeyPair/${Id}	aws:ResourceTag/${TagKey}
StaticIp	arn:${Partition}:lightsail:${Region}:${Account}:StaticIp/${Id}	aws:ResourceTag/${TagKey}
Disk	arn:${Partition}:lightsail:${Region}:${Account}:Disk/${Id}	aws:ResourceTag/${TagKey}
DiskSnapshot	arn:${Partition}:lightsail:${Region}:${Account}:DiskSnapshot/${Id}	aws:ResourceTag/${TagKey}
LoadBalancer	arn:${Partition}:lightsail:${Region}:${Account}:LoadBalancer/${Id}	aws:ResourceTag/${TagKey}
LoadBalancerTlsCertificate	arn:${Partition}:lightsail:${Region}:${Account}:LoadBalancerTlsCertificate/${Id}	
ExportSnapshotRecord	arn:${Partition}:lightsail:${Region}:${Account}:ExportSnapshotRecord/${Id}	
CloudFormationStackRecord	arn:${Partition}:lightsail:${Region}:${Account}:CloudFormationStackRecord/${Id}	

Ressourcentypen	ARN	Bedingungsschlüssel
RelationalDatabase	`arn:${Partition}:lightsail:${Region}:${Account}:RelationalDatabase/${Id}`	aws:ResourceTag/${TagKey}
RelationalDatabaseSnapshot	`arn:${Partition}:lightsail:${Region}:${Account}:RelationalDatabaseSnapshot/${Id}`	aws:ResourceTag/${TagKey}
Alarm	`arn:${Partition}:lightsail:${Region}:${Account}:Alarm/${Id}`	
Certificate	`arn:${Partition}:lightsail:${Region}:${Account}:Certificate/${Id}`	aws:ResourceTag/${TagKey}
ContactMethod	`arn:${Partition}:lightsail:${Region}:${Account}:ContactMethod/${Id}`	
ContainerService	`arn:${Partition}:lightsail:${Region}:${Account}:ContainerService/${Id}`	aws:ResourceTag/${TagKey}
Distribution	`arn:${Partition}:lightsail:${Region}:${Account}:Distribution/${Id}`	aws:ResourceTag/${TagKey}
Bucket	`arn:${Partition}:lightsail:${Region}:${Account}:Bucket/${Id}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Lightsail

Amazon Lightsail definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wertepaaren, die in der Anforderung zulässig sind	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paar einer Ressource	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach Liste von Tag-Schlüsseln, die in der Anforderung zulässig sind	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Location

Amazon Location (Servicepräfix: `geo`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Location definierte Aktionen
- Von Amazon Location definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Location

Von Amazon Location definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den

Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateTrackerConsumer	Gewährt die Berechtigung, eine Verknüpfung zwischen einer Geofence-Sammlung und einer Tracker-Ressource zu erstellen	Write	tracker*		
BatchDeleteDevicePositionHistory	Gewährt die Berechtigung zum Löschen eines Batch von Gerätepositionsverläufen aus einer Tracker-Ressource	Write	tracker*		
				geo:DeviceIds	
BatchDeleteGeofence	Gewährt die Berechtigung, einen Batch von Geofences aus einer Geofence-Sammlung zu löschen	Write	geofence-collection*		
				geo:GeofenceIds	
BatchEvaluateGeofences	Gewährt die Berechtigung, in einer bestimmten Geofence-Sammlung die Gerätepositionen gegenüber der Position von Geofences zu bewerten	Write	geofence-collection*		
BatchGetDevicePosition	Gewährt die Berechtigung zum Senden einer Batch-Anforderung zum Abrufen von Gerätepositionen	Read	tracker*		
				geo:DeviceIds	
BatchPutGeofence	Gewährt die Berechtigung zum Senden einer Batch-Anforderung zum Hinzufügen von	Write	geofence-collection*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Geofences zu einer bestimmten Geofence-Sammlung			geo:GeofenceIds	
BatchUpdateDevicePosition	Gewährt die Berechtigung zum Upload einer Positionsaktualisierung für ein oder mehrere Geräte auf eine Tracker-Ressource	Write	tracker*		
				geo:DeviceIds	
CalculateRoute	Gewährt die Berechtigung zum Berechnen von Routen mit einer bestimmten Routenrechner-Ressource	Lesen	route-calculator*		
CalculateRouteMatrix	Gewährt die Berechtigung zum Berechnen einer Route-Matrix mit einer bestimmten Routenrechner-Ressource	Lesen	route-calculator*		
CreateGeofenceCollection	Gewährt die Berechtigung zum Erstellen einer Geofence-Sammlung	Schreiben	geofence-collection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateKey	Gewährt die Berechtigung zum Erstellen einer API-Schlüsselressource	Schreiben	api-key*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMap	Gewährt die Berechtigung zum Erstellen einer Kartenressource	Write	map*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePlaceIndex	Gewährt die Berechtigung zum Erstellen einer Ortsindexressource	Write	place-index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRouteCalculator	Gewährt die Berechtigung zum Erstellen einer Routenrechner-Ressource	Write	route-calculator*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTracker	Gewährt die Berechtigung zum Erstellen einer Tracker-Ressource	Write	tracker*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteGeofenceCollection	Gewährt die Berechtigung zum Löschen einer Geofence-Sammlung	Schreiben	geofence-collection*		
DeleteKey	Gewährt die Berechtigung zum Löschen einer API-Schlüsselressource	Schreiben	api-key*		
DeleteMap	Gewährt die Berechtigung zum Löschen einer Kartenressource	Write	map*		
DeletePlaceIndex	Gewährt die Berechtigung zum Löschen einer Ortsindexressource	Write	place-index*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteRouteCalculator	Gewährt die Berechtigung zum Löschen einer Routenrechner-Ressource	Write	route-calculator*		
DeleteTracker	Gewährt die Berechtigung zum Löschen einer Tracker-Ressource	Write	tracker*		
DescribeGeofenceCollection	Gewährt die Berechtigung zum Abrufen von Details zu einer Geofence-Sammlung	Lesen	geofence-collection*		
DescribeKey	Gewährt die Berechtigung zum Abrufen von Details zu einer API-Schlüsselressource und Secrets	Lesen	api-key*		
DescribeMap	Gewährt die Berechtigung zum Abrufen von Details zu einer Kartenressource	Read	map*		
DescribePlaceIndex	Gewährt die Berechtigung zum Abrufen von Details zu einer Ortsindexressource	Read	place-index*		
DescribeRouteCalculator	Gewährt die Berechtigung zum Abrufen von Routenrechner-Ressourcendetails	Read	route-calculator*		
DescribeTracker	Gewährt die Berechtigung zum Abrufen von Details zu einer Tracker-Ressource	Read	tracker*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateTrackerConsumer	Gewährt die Berechtigung, die Verknüpfung zwischen einer Tracker-Ressource und einer Geofence-Sammlung zu entfernen	Write	tracker*		
GetDevicePosition	Gewährt die Berechtigung zum Abrufen der aktuellsten Geräteposition	Lesen	tracker*		
				geo:DeviceIds	
GetDevicePositionHistory	Gewährt die Berechtigung zum Abrufen des Gerätepositionsverlaufs	Lesen	tracker*		
				geo:DeviceIds	
GetGeofence	Gewährt die Berechtigung zum Abrufen von Geofence-Details zu einer Geofence-Sammlung	Lesen	geofence-collection*		
				geo:GeofenceIds	
GetMapGlyphs	Gewährt die Berechtigung zum Abrufen der Glyph-Datei für eine Kartenressource	Read	map*		
GetMapSprites	Gewährt die Berechtigung zum Abrufen der Sprite-Datei für eine Kartenressource	Read	map*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetMapStyleDescriptor	Gewährt die Berechtigung zum Abrufen der Kartenstil-Beschreibung aus einer Kartenressource	Read	map*		
GetMapTile	Gewährt die Berechtigung zum Abrufen der Kartenkachel aus der Kartenressource	Lesen	map*		
GetPlace	Gewährt die Berechtigung zum Finden eines Ortes anhand seiner eindeutigen ID	Lesen	place-index*		
ListDevicePositions	Gewährt die Erlaubnis zum Abrufen einer Liste von Geräten und ihren neuesten Positionen von der angegebenen Tracker-Ressource	Lesen	tracker*		
ListGeofenceCollections	Gewährt die Berechtigung zum Auflisten von Geofence-Sammlungen	List	geofence-collection*		
ListGeofences	Gewährt die Berechtigung zum Auflisten von Geofences, die in einer bestimmten Geofence-Sammlung gespeichert sind	Lesen	geofence-collection*		
ListKeys	Gewährt die Berechtigung zum Auflisten von API-Schlüsselressourcen	Auflisten	api-key*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListMaps	Gewährt die Berechtigung zum Auflisten von Kartenressourcen	List	map*		
ListPlaceIndexes	Gewährt die Berechtigung zum Aufrufen einer Liste von Ortsindexressourcen	List	place-index*		
ListRouteCalculators	Gewährt die Berechtigung zum Aufrufen einer Liste von Routenrechner-Ressourcen	List	route-calculator*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags (Metadaten), die Sie der Ressource zugewiesen haben	Read	api-key		
			geofence-collection		
			map		
			place-index		
			route-calculator		
			tracker		
ListTrackerConsumers	Gewährt die Berechtigung zum Abrufen einer Liste von Geofence-Sammlungen, die derzeit der angegebenen Tracker-Ressource zugeordnet sind	Read	tracker*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTrackers	Gewährt die Berechtigung zum Aufrufen einer Liste von Tracker-Ressourcen	List	tracker*		
PutGeofence	Gewährt die Berechtigung, einen neuen Geofence zu einer bestimmten Geofence-Sammlung hinzuzufügen oder einen vorhandenen Geofence zu aktualisieren	Write	geofence-collection*		
				geo:GeofenceIds	
SearchPlaceIndexForPosition	Gewährt die Berechtigung zum Umkehren der Geocodes einer bestimmten Koordinate	Lesen	place-index*		
SearchPlaceIndexForSuggestions	Erteilt die Erlaubnis, Vorschläge für Adressen und Interessenpunkte auf der Grundlage von teilweisem oder falsch geschriebenem Freiformtext zu generieren	Lesen	place-index*		
SearchPlaceIndexForText	Gewährt die Berechtigung zum Geocodieren von Freitext wie Adresse, Name, Ort oder Region	Read	place-index*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung, Tags zur angegebenen Ressource hinzuzufügen oder diese zu ändern. Tags sind Metadaten, die zur Verwaltung einer Ressource verwendet werden können.	Markieren	api-key		
			geofence-collection		
			map		
			place-index		
			route-calculator		
			tracker		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung, die angegebenen Tags (Metadaten) aus der Ressource zu entfernen	Markierung	api-key		
			geofence-collection		
			map		
			place-index		
			route-calculator		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			tracker		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateGeofenceCollection	Gewährt die Berechtigung zum Aktualisieren einer Geofence-Sammlung	Schreiben	geofence-collection*		
UpdateKey	Gewährt die Berechtigung zum Aktualisieren einer API-Schlüsselressource	Schreiben	api-key*		
UpdateMap	Gewährt die Berechtigung zum Aktualisieren einer Map-Ressource	Schreiben	map*		
UpdatePlaceIndex	Gewährt die Berechtigung zum Aktualisieren einer Ortsindexressource	Schreiben	place-index*		
UpdateRouteCalculator	Gewährt die Berechtigung zum Aktualisieren einer Routenrechner-Ressource	Schreiben	route-calculator*		
UpdateTracker	Gewährt die Berechtigung zum Aktualisieren einer Tracker-Ressource	Schreiben	tracker*		

Von Amazon Location definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
api-key	`arn:${Partition}:geo:${Region}:${Account}:api-key/${KeyName}`	aws:ResourceTag/${TagKey}
geofence-collection	`arn:${Partition}:geo:${Region}:${Account}:geofence-collection/${GeofenceCollectionName}`	aws:ResourceTag/${TagKey} geo:GeofenceIds
map	`arn:${Partition}:geo:${Region}:${Account}:map/${MapName}`	aws:ResourceTag/${TagKey}
place-index	`arn:${Partition}:geo:${Region}:${Account}:place-index/${IndexName}`	aws:ResourceTag/${TagKey}
route-calculator	`arn:${Partition}:geo:${Region}:${Account}:route-calculator/${CalculatorName}`	aws:ResourceTag/${TagKey}
tracker	`arn:${Partition}:geo:${Region}:${Account}:tracker/${TrackerName}`	aws:ResourceTag/${TagKey} geo:DeviceIds

Bedingungsschlüssel für Amazon Location

Amazon Location definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die

Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Schlüssel eines Tags und den Wert einer Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach den Tag-Schlüsseln in einer Anforderung	ArrayOfString
geo:DeviceIds	Filtert den Zugriff durch das Vorhandensein von Geräte-IDs in der Anforderung	ArrayOfString
geo:GeofenceIds	Filtert den Zugriff durch das Vorhandensein von Geofence-IDs in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Lookout for Equipment

Amazon Lookout for Equipment (Servicepräfix: `lookoutequipment`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Lookout for Equipment definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDataset	Gewährt die Berechtigung zum Erstellen eines Dataset	Write	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInferenceScheduler	Gewährt die Berechtigung zum Erstellen eines Inferenzschedulers für ein trainiertes Modell	Schreiben	inference-scheduler*		
			model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLabel	Gewährt die Berechtigung zum Erstellen einer Bezeichnung	Schreiben	label-group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateLabelGroup	Gewährt die Berechtigung zum Erstellen einer Bezeichnungsgruppe	Schreiben	label-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModel	Gewährt die Berechtigung zum Erstellen eines Modells, das für ein Dataset trainiert ist	Schreiben	dataset*		
			model*		
			label-group		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRetrainingScheduler	Gewährt die Berechtigung zum Erstellen eines Planers für das erneute Training eines trainierten Modells	Schreiben	model*		
DeleteDataset	Gewährt die Berechtigung zum Löschen eines Dataset	Write	dataset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteInferenceScheduler	Gewährt die Berechtigung zum Löschen eines Inferenzschedulers	Schreiben	inference-scheduler*		
DeleteLabel	Gewährt die Berechtigung zum Löschen einer Bezeichnung	Schreiben	label-group*		
DeleteLabelGroup	Gewährt die Berechtigung zum Löschen einer Bezeichnungsgruppe	Schreiben	label-group*		
DeleteModel	Gewährt die Berechtigung zum Löschen eines Trails	Schreiben	model*		
DeleteResourcePolicy	Gewährt die Berechtigung zum Löschen einer Ressourcenrichtlinie	Schreiben	dataset		
			model		
			model-version		
DeleteRetrainingScheduler	Gewährt die Berechtigung zum Löschen eines Planers für das erneute Training eines trainierten Modells	Schreiben	model*		
DescribeDataIngestionJob	Gewährt die Berechtigung, einen Dateneingabejob zu beschreiben	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDataset	Gewährt die Berechtigung zum Beschreiben eines Dataset	Read	dataset*		
DescribeInferenceScheduler	Gewährt die Berechtigung zur Beschreibung eines Inferenzschedulers	Lesen	inference-scheduler*		
DescribeLabelGroup	Gewährt die Berechtigung zum Beschreiben einer Bezeichnungsgruppe	Lesen	label-group*		
DescribeModel	Gewährt die Berechtigung zum Beschreiben eines Modells	Lesen	model*		
DescribeModelVersion	Erteilt die Berechtigung zum Beschreiben einer Modellversion	Lesen	model-version*		
DescribeResourcePolicy	Erteilt die Berechtigung zum Beschreiben einer Ressourcenrichtlinie	Lesen	dataset		
			model		
			model-version		
DescribeRetrainingScheduler	Gewährt die Berechtigung zum Beschreiben eines Planers für das erneute Training eines trainierten Modells	Lesen	model*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeLabel	Gewährt die Berechtigung zum Beschreiben einer Bezeichnung	Lesen	label-group*		
ImportDataset	Erteilt die Berechtigung zum Importieren eines Datasets	Schreiben	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ImportModelVersion	Erteilt die Berechtigung zum Importieren einer Modellversion.	Schreiben	dataset*		
			model*		
			label-group		
				aws:RequestTag/${TagKey} aws:TagKeys lookoutequipment:IsImportingData	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDataIngestionJobs	Gewährt die Berechtigung zum Auflisten der Dateneingabejobs in Ihrem Konto oder für einen bestimmten Datensatz	List	dataset*		
ListDatasets	Gewährt die Berechtigung zum Auflisten der Datensätze in Ihrem Konto	Auflisten			
ListInferenceEvents	Gewährt die Berechtigung zum Auflisten der Inferenzereignisse für einen Inferenzscheduler	Lesen	inference-scheduler*		
ListInferenceExecutions	Gewährt die Berechtigung zum Auflisten der Inferenzausführungen für einen Inferenzschedulers	Read	inference-scheduler*		
ListInferenceSchedulers	Gewährt die Berechtigung zum Auflisten der Inferenzplaner in Ihrem Konto	Auflisten			
ListLabelGroups	Gewährt die Berechtigung zum Auflisten der Bezeichnungsgruppen in Ihrem Konto	Auflisten	label-group*		
ListLabels	Gewährt die Berechtigung zum Auflisten der Bezeichnungen in Ihrem Konto	Auflisten	label-group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListModelVersions	Erteilt die Berechtigung zum Auflisten der Modellversionen in Ihrem Konto	Auflisten	model*		
ListModels	Gewährt die Berechtigung zum Auflisten der Modelle in Ihrem Konto	Auflisten			
ListRetrainingSchedulers	Gewährt die Berechtigung zum Auflisten des Planers für das erneute Training in Ihrem Konto	Auflisten			
ListSensorStatistics	Gewährt die Berechtigung zum Auflisten der Sensorstatistiken für einen bestimmten Datensatz oder einen Erfassungsjob	Auflisten	dataset*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für eine Ressource	Lesen	dataset		
			inference-scheduler		
			label-group		
			model		
			model-version		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutResourcePolicy	Erteilt die Berechtigung zum Festlegen einer Ressourcenrichtlinie	Schreiben	dataset		
			model		
			model-version		
StartDataIngestionJob	Gewährt die Berechtigung zum Starten eines Datenaufnahme-Auftrags für einen Datensatz	Write	dataset*		
StartInferenceScheduler	Gewährt die Berechtigung zum Starten eines Inferenzschedulers	Schreiben	inference-scheduler*		
StartRetrainingScheduler	Gewährt die Berechtigung zum Starten eines Planers für das erneute Training eines trainierten Modells	Schreiben	model*		
StopInferenceScheduler	Gewährt die Berechtigung zum Stoppen eines Inferenzschedulers	Schreiben	inference-scheduler*		
StopRetrainingScheduler	Gewährt die Berechtigung zum Stoppen eines Planers für das erneute Training eines trainierten Modells	Schreiben	model*		
TagResource		Markieren	dataset		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags		inference-scheduler		
			label-group		
			model		
			model-version		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Markierung	dataset		
			inference-scheduler		
			label-group		
			model		
			model-version		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
UpdateActiveModelVersion	Erteilt die Berechtigung, die aktive Modellversion für ein bestimmtes Machine-Learning-Modell festzulegen	Schreiben	model*		
			model-version*		
UpdateInferenceScheduler	Gewährt die Berechtigung zum Aktualisieren eines Inferenzschedulers	Schreiben	inference-scheduler*		
UpdateLabelGroup	Gewährt die Berechtigung zum Aktualisieren einer Bezeichnungsgruppe	Schreiben	label-group*		
UpdateModel	Gewährt die Berechtigung zum Aktualisieren eines trainierten Modells	Schreiben	model*		
UpdateRetrainingScheduler	Gewährt die Berechtigung zum Aktualisieren eines Planers für das erneute Training eines trainierten Modells	Schreiben	model*		

Von Amazon Lookout for Equipment definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
dataset	`arn:${Partition}:lookoutequipment:${Region}:${Account}:dataset/${DatasetName}/${DatasetId}`	aws:ResourceTag/${TagKey}
model	`arn:${Partition}:lookoutequipment:${Region}:${Account}:model/${ModelName}/${ModelId}`	aws:ResourceTag/${TagKey}
model-version	`arn:${Partition}:lookoutequipment:${Region}:${Account}:model/${ModelName}/${ModelId}/model-version/${ModelVersionNumber}`	aws:ResourceTag/${TagKey}
inference-scheduler	`arn:${Partition}:lookoutequipment:${Region}:${Account}:inference-scheduler/${InferenceSchedulerName}/${InferenceSchedulerId}`	aws:ResourceTag/${TagKey}
label-group	`arn:${Partition}:lookoutequipment:${Region}:${Account}:label-group/${LabelGroupName}/${LabelGroupId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Lookout for Equipment

Amazon Lookout for Equipment definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString
lookoutequipment:IsImportingData	Filtert den Zugriff nach der Importstrategie der zugrunde liegenden Daten	Bool

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Lookout for Metrics

Amazon Lookout for Metrics (Servicepräfix: `lookoutmetrics`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Lookout for Metrics definierte Aktionen
- Von Amazon Lookout for Metrics definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Lookout for Metrics

Von Amazon Lookout for Metrics definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ActivateAnomalyDetector	Gewährt die Berechtigung zur Aktivierung eines Anomaliedetektors	Write	AnomalyDetector*		
BackTestAnomalyDetector	Gewährt die Berechtigung, einen Backtest mit einem Anomaliedetektor durchzuführen	Write	AnomalyDetector*		
CreateAlert	Gewährt die Berechtigung, eine Warnung für einen Anomaliedetektor zu erstellen	Write	Alert*		
			AnomalyDetector*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAnomalyDetector	Gewährt die Berechtigung zum Erstellen eines Anomaliedetektors	Write	AnomalyDetector*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMetricSet	Gewährt die Berechtigung zum Erstellen eines Dataset	Schreiben	AnomalyDetector*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			MetricSet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeactivateAnomalyDetector	Gewährt die Berechtigung zur Deaktivierung eines Anomaliedetektors	Schreiben	AnomalyDetector*		
DeleteAlert	Gewährt die Berechtigung zum Löschen einer Warnung	Write	Alert*		
DeleteAnomalyDetector	Gewährt die Berechtigung zum Löschen eines Anomaliedetektors	Write	AnomalyDetector*		
DescribeAlert	Gewährt die Berechtigung zum Abrufen von Details über eine Warnung	Read	Alert*		
DescribeAnomalyDetectionExecutions	Gewährt die Berechtigung, Informationen über eine Aufgabe zur Anomaliedetektion zu erhalten	Read	AnomalyDetector*		
DescribeAnomalyDetector	Gewährt die Berechtigung, Details zu einem Anomaliedetektor zu erhalten	Read	AnomalyDetector*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeMetricSet	Gewährt die Berechtigung zum Abrufen von Details zu einem Dataset	Lesen	MetricSet*		
DetectMetricSetConfig	Gewährt die Berechtigung zum Erkennen der Metriksatzkonfiguration aus der Datenquelle	Schreiben	AnomalyDetector*		
GetAnomalyGroup	Gewährt die Berechtigung, Details zu einer Gruppe von betroffenen Metriken zu erhalten	Read	AnomalyDetector*		
GetDataQualityMetrics	Gewährt die Berechtigung, Datenqualitätsmetriken für einen Anomaliedetektor zu erhalten	Read	AnomalyDetector*		
GetFeedback	Gewährt die Berechtigung, Feedback zu betroffenen Metriken für eine Anomaliegruppe zu erhalten	Read	AnomalyDetector*		
GetSampleData	Gewährt die Berechtigung, eine Auswahl von Beispieldatensätzen aus einer Amazon-S3-Datenquelle zu erhalten	Read			
ListAlerts	Gewährt die Berechtigung, eine Liste von Warnungen für einen Detektor zu erhalten	List	AnomalyDetector		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAnomalyDetectors	Gewährt die Berechtigung, eine Liste von Anomalied etektoren zu erhalten	Auflisten			
ListAnomalyGroupRelatedMetrics	Gewährt die Berechtigung, eine Liste ähnlicher Maßnahmen in einer Anomaliegruppe zu erhalten	Auflisten	AnomalyDetector*		
ListAnomalyGroupSummaries	Gewährt die Berechtigung, eine Liste von Anomaliegruppen zu erhalten	List	AnomalyDetector*		
ListAnomalyGroupTimeSeries	Gewährt die Berechtigung, eine Liste der betroffenen Metriken für eine Maßnahme in einer Anomaliegruppe zu erhalten	List	AnomalyDetector*		
ListMetricSets	Gewährt die Berechtigung zum Abrufen einer Liste von Datasets	List	AnomalyDetector		
ListTagsForResource	Gewährt die Erlaubnis, eine Liste von Tags für einen Detektor, einen Datensatz oder eine Warnung zu erhalten	Read	Alert		
			AnomalyDetector		
			MetricSet		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutFeedback	Gewährt die Berechtigung zum Hinzufügen von Feedback für eine betroffene Metrik in einer Anomaliegruppe	Write	AnomalyDetector*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einem Detektor, einem Datensatz oder einer Warnung	Markieren	Alert		
			AnomalyDetector		
			MetricSet		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags von einem Detektor, einem Datensatz oder einer Warnung	Markierung	Alert		
			AnomalyDetector		
			MetricSet		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateAlert	Gewährt die Berechtigung zum Aktualisieren einer Warnung für einen Anomaliedetektor	Schreiben	Alert*		
UpdateAnomalyDetector	Gewährt die Berechtigung, einen Anomaliedetektor zu aktualisieren	Write	AnomalyDetector*		
UpdateMetricSet	Gewährt die Berechtigung zum Aktualisieren eines Dataset	Write	MetricSet*		

Von Amazon Lookout for Metrics definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
AnomalyDetector	`arn:${Partition}:lookoutmetrics:${Region}:${Account}:AnomalyDetector:${AnomalyDetectorName}`	aws:ResourceTag/${TagKey}
MetricSet	`arn:${Partition}:lookoutmetrics:${Region}:${Account}:MetricSet/${AnomalyDetectorName}/${MetricSetName}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
Alert	`arn:${Partition}:lookoutmetrics:${Region}:${Account}:Alert:${AlertName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Lookout for Metrics

Amazon Lookout for Metrics definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Lookout for Vision

Amazon Lookout for Vision (Servicepräfix: `lookoutvision`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Lookout for Vision definierte Aktionen
- Von Amazon Lookout for Vision definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Lookout for Vision

Von Amazon Lookout for Vision definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDataset	Gewährt die Berechtigung zum Erstellen eines Dataset-Manifests	Write			
CreateModel	Gewährt die Berechtigung zum Erstellen eines neuen Anomalieerkennungsmodells	Write	model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProject	Gewährt die Berechtigung zum Erstellen eines neuen Projekts	Write	project*		
DeleteDataset	Gewährt die Berechtigung zum Löschen eines Dataset	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteModel	Gewährt die Berechtigung zum Löschen eines Modells und aller zugehörigen Assets	Write	model*		
DeleteProject	Gewährt die Berechtigung zum dauerhaften Entfernen eines Projekts	Write	project*		
DescribeDataset	Gewährt die Berechtigung, detaillierte Informationen zum Dataset-Manifest anzuzeigen	Read			
DescribeModel	Gewährt die Berechtigung, detaillierte Informationen zu einem Modell anzuzeigen	Lesen	model*		
DescribeModelPackagingJob	Gewährt die Berechtigung, detaillierte Informationen zu einem Modellpaketauftrag anzuzeigen	Lesen			
DescribeProject	Gewährt die Berechtigung, detaillierte Informationen zu einem Projekt anzuzeigen	Read	project*		
DescribeTrialDetection [nur Berechtigung]	Gewährt die Berechtigung, Statusinformationen zu einer ausgeführten Anomaliee rkennungsaufgabe bereitzustellen	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DetectAnomalies	Gewährt die Berechtigung zum Aufrufen der Erkennung von Anomalien	Write	model*		
ListDatasetEntries	Gewährt die Berechtigung zum Auflisten der Inhalte des Dataset-Manifests aufzulisten	Lesen			
ListModelPackagingJobs	Gewährt die Berechtigung zum Auflisten aller Modelpaketaufträge, die einem Projekt zugeordnet sind	Auflisten			
ListModels	Gewährt die Berechtigung zum Auflisten aller Modelle, die einem Projekt zugeordnet sind	List			
ListProjects	Gewährt die Berechtigung zum Auflisten aller Projekte	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen	model		
ListTrialDetections [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aller Anomalieerkennungsaufgaben	List			
StartModel	Gewährt die Berechtigung zum Starten des Anomalieerkennungsmodells	Schreiben	model*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartModelPackagingJob	Gewährt die Berechtigung zum Starten eines Modellpaketauftrags	Schreiben	model*		
StartTrialDetection [nur Berechtigung]	Gewährt die Berechtigung zum Starten der Massenerkennung von Anomalien für einen Satz von Bildern, die in einem S3 Bucket gespeichert sind	Write			
StopModel	Gewährt die Berechtigung zum Beenden des Anomaliee rkennungsmodells	Schreiben	model*		
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit bestimmten Schlüsselwertpaaren	Markierung	model		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung, das Tag mit dem angegebenen Schlüssel aus einer Ressource zu entfernen	Markierung	model		
				aws:TagKeys	
UpdateDatasetEntries	Gewährt die Berechtigung zum Aktualisieren eines Trainings- oder Test-Dataset-Manifests	Write			

Von Amazon Lookout for Vision definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
model	`arn:${Partition}:lookoutvision:${Region}:${Account}:model/${ProjectName}/${ModelVersion}`	aws:ResourceTag/${TagKey}
project	`arn:${Partition}:lookoutvision:${Region}:${Account}:project/${ProjectName}`	

Bedingungsschlüssel für Amazon Lookout for Vision

Amazon Lookout for Vision definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Machine Learning

Amazon Machine Learning (Servicepräfix: `machinelearning`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Machine Learning definierte Aktionen
- Von Amazon Machine Learning definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Machine Learning

Von Amazon Machine Learning definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddTags	Fügt einem Objekt ein oder mehrere Tags (maximal 10)	Markieren	batchprediction		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	hinzu. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert		datasource		
			evaluation		
			mlmodel		
CreateBatchPrediction	Generiert Prognosen für eine Gruppe von Beobachtungen.	Write	batchprediction*		
			datasource*		
			mlmodel*		
CreateDataSourceFromRDS	Erstellt ein DataSource-Objekt aus einem Amazon RDS.	Write	datasource*		
CreateDataSourceFromRedshift	Erstellt eine DataSource aus einer Datenbank, die auf einem Amazon Redshift-Cluster gehostet wird.	Write	datasource*		
CreateDataSourceFromS3	Erstellt ein DataSource-Objekt aus S3.	Write	datasource*		
CreateEvaluation	Erstellt eine neue Bewertung eines MLModel.	Write	datasource*		
			evaluation*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			mlmodel*		
CreateMLModel	Erstellt ein neues MLModel.	Write	datasource*		
			mlmodel*		
CreateRealtimeEndpoint	Erstellt einen Echtzeit-Endpunkt für das MLModel.	Write	mlmodel*		
DeleteBatchPrediction	Weist den Status DELETED einer BatchPrediction zu und macht sie so unbrauchbar.	Write	batchprediction*		
DeleteDataSource	Weist den Status DELETED einer DataSource zu und macht sie so unbrauchbar.	Write	datasource*		
DeleteEvaluation	Weist den Status DELETED einer Bewertung zu und macht sie so unbrauchbar.	Write	evaluation*		
DeleteMLModel	Weist den Status DELETED einem MLModel zu und macht es so unbrauchbar.	Write	mlmodel*		
DeleteRealtimeEndpoint	Löscht einen Echtzeit-Endpunkt eines MLModel.	Write	mlmodel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteTags	Löscht die angegebenen Tags, die einem ML-Objekt zugeordnet sind. Nachdem diese Produktion abgeschlossen ist, können Sie keine gelöschten Tags wiederherstellen.	Markieren	batchprediction		
			datasource		
			evaluation		
			mlmodel		
DescribeBatchPredictions	Gibt eine Liste der BatchPrediction-Produktionen zurück, die den Suchkriterien in der Anforderung entsprechen.	List			
DescribeDataSources	Gibt eine Liste der DataSource-Objekte zurück, die den Suchkriterien in der Anforderung entsprechen.	List			
DescribeEvaluations	Gibt eine Liste der DescribeEvaluations zurück, die den Suchkriterien in der Anforderung entsprechen.	List			
DescribeMLModels	Gibt eine Liste der MLModel-Objekte zurück, die den Suchkriterien in der Anforderung entsprechen.	List			
DescribeTags	Beschreibt ein oder mehrere Tags für Ihr Amazon ML-Objekt.	List	batchprediction		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			datasource		
			evaluation		
			mlmodel		
GetBatchPrediction	Gibt eine BatchPrediction mit detaillierten Metadaten, Status und Datendateiinformationen zurück.	Read	batchprediction*		
GetDataSource	Gibt eine DataSource mit Metadaten und Datendateiinformationen sowie den aktuellen Status der DataSource zurück.	Read	datasource*		
GetEvaluation	Gibt eine Bewertung mit Metadaten sowie den aktuellen Status der Bewertung zurück.	Read	datasource*		
GetMLModel	Gibt ein MLModel mit detaillierten Metadaten und Datenquellinformationen sowie den aktuellen Status des MLModel zurück.	Read	mlmodel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Predict	Generiert eine Prognose für die Beobachtung unter Verwendung des angegebenen ML-Modells.	Write	mlmodel*		
UpdateBatchPrediction	Aktualisiert den BatchPredictionName einer BatchPrediction.	Write	batchprediction*		
UpdateDataSource	Aktualisiert den DataSourceName einer DataSource.	Write	datasource*		
UpdateEvaluation	Aktualisiert den EvaluationName einer Bewertung.	Write	evaluation*		
UpdateMLModel	Aktualisiert den MLModelName und den ScoreThreshold eines MLModel.	Write	mlmodel*		

Von Amazon Machine Learning definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
batchprediction	`arn:${Partition}:machinelearning:${Region}:${Account}:batchprediction/${BatchPredictionId}`	
datasource	`arn:${Partition}:machinelearning:${Region}:${Account}:datasource/${DatasourceId}`	
evaluation	`arn:${Partition}:machinelearning:${Region}:${Account}:evaluation/${EvaluationId}`	
mlmodel	`arn:${Partition}:machinelearning:${Region}:${Account}:mlmodel/${MlModelId}`	

Bedingungsschlüssel für Amazon Machine Learning

Machine Learning umfasst keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Macie

Amazon Macie (Servicepräfix: `macie2`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Macie definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

> **Note**
>
> Die Aktionen DisassociateFromMasterAccount und GetMasterAccount sind veraltet. Es wird empfohlen, die Aktionen DisassociateFromAdministratorAccount und GetAdministratorAccount anzugeben.

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptInvitation	Gewährt die Berechtigung, eine Amazon Macie Mitgliedschaftseinladung anzunehmen.	Write			
BatchGetCustomDataIdentifiers	Gewährt die Berechtigung zum Abrufen von Informationen über einen oder mehrere benutzerdefinierte Datenbezeichner.	Lesen	CustomDataIdentifier*		
CreateAllowList	Gewährt die Berechtigung zum Erstellen und Definieren der Einstellungen für eine Zulassungsliste	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateClassificationJob	Gewährt die Berechtigung zum Erstellen und Definieren der Einstellungen für	Write	ClassificationJob*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	einen sensiblen Datenerkennungsauftrag			aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomDataIdentifier	Gewährt die Berechtigung zum Erstellen und Definieren der Einstellungen für einen benutzerdefinierten Datenbezeichner.	Write	CustomDataIdentifier*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFindingsFilter	Gewährt die Berechtigung zum Erstellen und Definieren der Einstellungen für einen Ergebnisfilter.	Write	FindingsFilter*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInvitations	Gewährt die Berechtigung zum Senden einer Amazon Macie-Mitgliedschaftseinladung.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateMember	Gewährt die Berechtigung, ein Konto einem Amazon-Macie-Administrator-Konto zuzuordnen.	Write	Member*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSampleFindings	Gewährt die Berechtigung zum Erstellen von Beispielergebnissen.	Write			
DeclineInvitations	Gewährt die Berechtigung zum Ablehnen von Amazon Macie-Mitgliedschaftseinladungen.	Schreiben			
DeleteAllowList	Gewährt die Berechtigung zum Löschen einer Zulassungsliste	Schreiben	AllowList*		
DeleteCustomDataIdentifier	Gewährt die Berechtigung zum Löschen eines benutzerdefinierten Datenbezeichners.	Write	CustomDataIdentifier*		
DeleteFindingsFilter	Gewährt die Berechtigung zum Löschen eines Ergebnisfilters.	Write	FindingsFilter*		
DeleteInvitations	Gewährt die Berechtigung zum Löschen von Amazon Macie-Mitgliedschaftseinladungen.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteMember	Gewährt die Berechtigung zum Löschen der Mapping zwischen einem Amazon-Macie-Administrator-Konto und einem Konto.	Write	Member*		
DescribeBuckets	Gewährt die Berechtigung zum Abrufen statistischer Daten und anderer Informationen zu S3-Buckets, die Amazon Macie überwacht und analysiert.	Read			
DescribeClassificationJob	Gewährt die Berechtigung zum Abrufen von Informationen über den Status und Einstellungen für einen Erkennungsauftrag für sensible Daten	Read	ClassificationJob*		
DescribeOrganizationConfiguration	Erteilung der Berechtigung zum Abrufen von Informationen über die Amazon-Macie-Konfigurationseinstellungen für eine AWS-Organisation	Read			
DisableMacie	Gewährt die Berechtigung zum Deaktivieren eines Amazon Macie-Kontos, wodurch auch Macie-Ressourcen für das Konto gelöscht werden.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisableOrganizationAdminAccount	Erteilung der Berechtigung, ein Konto als delegiertes Amazon-Macie-Administratorkonto für eine AWS-Organisation zu deaktivieren	Schreiben			
DisassociateFromAdministratorAccount	Erteilt einem Amazon-Macie-Mitgliedskonto die Berechtigung, die Zuordnung zu seinem Macie-Administratorkonto aufzuheben	Schreiben			
DisassociateFromMasterAccount	Erteilt einem Amazon-Macie-Mitgliedskonto die Berechtigung, die Zuordnung zu seinem Macie-Administratorkonto aufzuheben	Schreiben			
DisassociateMember	Gewährt einem Amazon-Macie-Administratorkonto die Berechtigung, die Verknüpfung mit seinem Macie-Mitgliedskonto aufzuheben	Schreiben	Member*		
EnableMacie	Gewährt die Berechtigung zum Aktivieren und Festlegen der Konfigurationseinstellungen für ein neues Amazon Macie-Konto.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
EnableOrganizationAdminAccount	Erteilung der Berechtigung, ein Konto als delegiertes Amazon-Macie-Administratorkonto für eine AWS-Organisation zu aktivieren	Write			
GetAdministratorAccount	Gewährt die Berechtigung zum Abrufen von Informationen über das Amazon-Macie-Administratorkonto für ein Konto	Lesen			
GetAllowList	Gewährt die Berechtigung zum Abrufen der Einstellungen und Status einer Zulassungsliste	Lesen	AllowList*		
GetAutomatedDiscoveryConfiguration	Gewährt die Berechtigung zum Abrufen der Konfigurationseinstellungen und Status der automatisierten Erkennung sensibler Daten für ein Konto	Lesen			
GetBucketStatistics	Gewährt die Berechtigung zum Abrufen aggregierter statistischer Daten für alle S3-Buckets, die Amazon Macie überwacht und analysiert.	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetClassificationExportConfiguration	Gewährt die Berechtigung zum Abrufen der Einstellungen zum Exportieren von Erkennungsergebnissen von sensiblen Daten.	Lesen			
GetClassificationScope	Gewährt die Berechtigung zum Abrufen der Klassifizierungsbereichseinstellungen für ein Konto	Lesen			
GetCustomDataIdentifier	Gewährt die Berechtigung zum Abrufen von Informationen zu den Einstellungen für einen benutzerdefinierten Datenbezeichner	Read	CustomDataIdentifier*		
GetFindingStatistics	Gewährt die Berechtigung zum Abrufen aggregierter statistischer Daten zu Ergebnissen.	Read			
GetFindings	Gewährt die Berechtigung zum Abrufen der Details eines oder mehrerer Ergebnisse	Read			
GetFindingsFilter	Gewährt die Berechtigung zum Abrufen von Informationen zu den Einstellungen für einen Ergebnisfilter	Read	FindingsFilter*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetFindingsPublicationConfiguration	Erteilung der Berechtigung zum Abrufen der Konfigurationseinstellungen für die Veröffentlichung von Ergebnissen in AWS Security Hub	Read			
GetInvitationsCount	Gewährt die Berechtigung zum Abrufen der Anzahl der Amazon Macie-Mitgliedschaftseinladungen, die von einem Konto empfangen wurden.	Read			
GetMacieSession	Gewährt die Berechtigung zum Abrufen von Informationen zu den Status- und Konfigurationseinstellungen für ein Amazon Macie-Konto	Lesen			
GetMasterAccount	Gewährt die Berechtigung zum Abrufen von Informationen über das Amazon-Macie-Administratorkonto für ein Konto	Lesen			
GetMember	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Konto, das mit einem Amazon Macie-Administrator-Konto verknüpft ist	Lesen	Member*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetResourceProfile	Gewährt die Berechtigung zum Abrufen von Statistiken zur Erkennung vertraulicher Daten und den Sensitivitätswert für einen S3-Bucket	Lesen			
GetRevealConfiguration	Erteilung der Berechtigung zum Abruf des Status und der Konfigurationseinstellungen für den Abruf von durch Befunde gemeldeten Vorkommnissen sensibler Daten	Lesen			
GetSensitiveDataOccurrences	Erteilung der Berechtigung zum Abrufen von Vorkommen sensibler Daten, die von einem Befund gemeldet wurden	Lesen			
GetSensitiveDataOccurrencesAvailability	Erteilung der Berechtigung zur Prüfung, ob Vorkommen sensibler Daten für einen Befund abgerufen werden können	Lesen			
GetSensitivityInspectionTemplate	Gewährt die Berechtigung zum Abrufen der Einstellungen für die Sensibilitätsprüfung für ein Konto	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetUsageStatistics	Gewährt die Berechtigung zum Abrufen von Kontingenten und aggregierten Nutzungsdaten für ein oder mehrere Konten.	Read			
GetUsageTotals	Gewährt die Berechtigung zum Abrufen aggregierter Nutzungsdaten für ein Konto.	Lesen			
ListAllowLists	Gewährt die Berechtigung zum Abrufen einer Teilmenge von Informationen zu allen Zulassungslisten für ein Konto	Auflisten			
ListClassificationJobs	Gewährt die Berechtigung zum Abrufen einer Teilmenge von Informationen über den Status und Einstellungen für einen oder mehrere Erkennungsaufträge für sensible Daten.	Auflisten			
ListClassification Scopes	Gewährt die Berechtigung zum Abrufen einer Teilmenge von Informationen zu allen Klassifizierungsbereichen für ein Konto	Auflisten			
ListCustomDataIdentifiers	Gewährt die Berechtigung zum Abrufen von Informationen über alle benutzerdefinierten Datenbezeichner	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListFindings	Gewährt die Berechtigung zum Abrufen einer Teilmenge von Informationen zu einem oder mehreren Ergebnissen.	List			
ListFindingsFilters	Gewährt die Berechtigung zum Abrufen von Informationen über alle Ergebnisfilter	List			
ListInvitations	Gewährt die Berechtigung zum Abrufen von Informationen über alle Amazon Macie-Mitgliedschaftseinladungen, die von einem Konto erhalten wurden	Auflisten			
ListManagedDataIdentifiers	Gewährt die Berechtigung zum Abrufen von Informationen zu verwalteten Datenkennungen	Auflisten			
ListMembers	Gewährt die Berechtigung zum Abrufen von Informationen über Konten, die mit einem Amazon-Macie-Administrator-Konto verknüpft sind	List			
ListOrganizationAdminAccounts	Erteilung der Berechtigung zum Abrufen von Informationen über das delegierte Amazon-Macie-Administratorkonto für eine AWS-Organisation	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListResourceProfileArtifacts	Gewährt die Berechtigung zum Abrufen von Informationen zu Objekten, die für die automatische Erkennung sensibler Daten aus einem S3-Buckets	Auflisten			
ListResourceProfileDetections	Gewährt die Berechtigung zum Abrufen von Informationen zu den Arten und Mengen der sensiblen Daten, die Amazon Macie in einem S3-Buckets gefunden hat	Auflisten			
ListSensitivityInspectionTemplates	Gewährt die Berechtigung zum Abrufen einer Teilmenge der Informationen über die Sensibilitätsprüfung für ein Konto	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Abrufen der Tags für eine Amazon-Macie-Ressource.	Read	AllowList		
			ClassificationJob		
			CustomDataIdentifier		
			FindingsFilter		
			Member		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutClassificationExportConfiguration	Gewährt die Berechtigung zum Erstellen oder Aktualisieren der Einstellungen zum Speichern von sensiblen Datenermittlungen	Write			
PutFindingsPublicationConfiguration	Erteilung der Berechtigung zur Aktualisierung der Konfigurationseinstellungen für die Veröffentlichung von Ergebnissen in AWS Security Hub	Write			
SearchResources	Erteilung der Berechtigung zum Abruf von statistischen Daten und anderen Informationen über AWS-Ressourcen, die Amazon Macie überwacht und analysiert	Read			
TagResource	Gewährt die Berechtigung zum Hinzufügen oder Aktualisieren der Tags für eine Amazon-Macie-Ressource	Markieren	AllowList		
			ClassificationJob		
			CustomDataIdentifier		
			FindingsFilter		
			Member		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
TestCustomDataIdentifier	Gewährt die Berechtigung zum Testen eines benutzerdefinierten Datenbezeichners.	Write			
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Amazon-Macie-Ressource.	Markierung	AllowList		
			ClassificationJob		
			CustomDataIdentifier		
			FindingsFilter		
			Member		
				aws:TagKeys	
UpdateAllowList	Erteilt die Berechtigung zum Aktualisieren der Einstellungen für eine Zulassungsliste	Schreiben	AllowList*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateAutomatedDiscoveryConfiguration	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren der automatischen Erkennung sensibler Daten für ein Konto	Schreiben			
UpdateClassificationJob	Gewährt die Berechtigung zum Ändern des Status eines Erkennungsauftrags für sensible Daten	Schreiben	ClassificationJob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateClassificationScope	Gewährt die Berechtigung zum Aktualisieren der Einstellungen für den Klassifizierungsumfang für ein Konto	Schreiben			
UpdateFindingsFilter	Gewährt die Berechtigung zum Aktualisieren der Einstellungen für einen Ergebnisfilter.	Write	FindingsFilter*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateMacieSession	Gewährt die Berechtigung, ein Amazon Macie-Konto auszusetzen oder erneut zu aktivieren oder die Konfigurationseinstellungen für ein Macie-Konto zu aktualisieren.	Schreiben			
UpdateMemberSession	Gewährt einem Amazon-Macie-Administrator-Konto die Berechtigung, ein Macie-Mitgliedskonto zu sperren oder wieder zu aktivieren	Schreiben			
UpdateOrganizationConfiguration	Erteilung der Berechtigung zur Aktualisierung der Amazon-Macie-Konfigurationseinstellungen für eine AWS Organisation	Schreiben			
UpdateResourceProfile	Gewährt die Berechtigung zum Aktualisieren der Sensitivitätsbewertung für ein S3-Buckets	Schreiben			
UpdateResourceProfileDetections	Gewährt die Berechtigung zum Aktualisieren der Sensitivitäts-Bewertungs-Einstellungen für ein S3-Buckets	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateRevealConfiguration	Erteilung der Berechtigung zur Aktualisierung der Status- und Konfigurationseinstellungen für den Abruf von durch Befunde gemeldeten Vorkommnissen sensibler Daten	Schreiben			
UpdateSensitivityInspectionTemplate	Gewährt die Berechtigung zum Aktualisieren der Einstellungen für die Sensibilitätsprüfung für ein Konto	Schreiben			

Von Amazon Macie definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
AllowList	`arn:${Partition}:macie2:${Region}:${Account}:allow-list/${ResourceId}`	aws:ResourceTag/${TagKey}
ClassificationJob	`arn:${Partition}:macie2:${Region}:${Account}:classification-job/${ResourceId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
CustomDataIdentifier	`arn:${Partition}:macie2:${Region}:${Account}:custom-data-identifier/${ResourceId}`	aws:ResourceTag/${TagKey}
FindingsFilter	`arn:${Partition}:macie2:${Region}:${Account}:findings-filter/${ResourceId}`	aws:ResourceTag/${TagKey}
Member	`arn:${Partition}:macie2:${Region}:${Account}:member/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Macie

Amazon Macie definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wertepaaren, die in der Anforderung zulässig sind	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paar einer Ressource	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS -Mainframe-Modernisierungsservice

AWS Der Mainframe Modernization Service (Dienstpräfix:`m2`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS -Mainframe-Modernisierungsservice definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelBatchJobExecution	Gewährt die Berechtigung zum Abbrechen der Ausführung eines Batch-Jobs	Schreiben	Application*		
CreateApplication	Gewährt die Berechtigung zum Erstellen einer Anwendung	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject s3:ListBucket

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDataSetImportTask	Gewährt die Berechtigung zum Erstellen einer Datensatz-Importaufgabe	Schreiben	Application*		s3:GetObject
CreateDeployment	Gewährt die Berechtigung zum Erstellen einer Bereitstellung	Schreiben	Application*		elasticloadbalancing:AddTags elasticloadbalancing:CreateListener elasticloadbalancing:CreateTargetGroup elasticloadbalancing:RegisterTargets
			Environment		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateEnvironment	Gewährt die Berechtigung zum Erstellen einer Umgebung	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcs ec2:ModifyNetworkInterfaceAttribute

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					elasticfilesystem:DescribeMountTargets elasticloadbalancing:AddTags elasticloadbalancing:CreateLoadBalancer fsx:DescribeFileSystems iam:CreateServiceLinkedRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteApplication	Gewährt die Berechtigung zum Löschen einer Anwendung	Schreiben	Application*		elasticloadbalancing:DeleteListener elasticloadbalancing:DeleteTargetGroup
DeleteApplicationFromEnvironment	Gewährt die Berechtigung zum Löschen einer Anwendung aus einer Laufzeitumgebung	Schreiben	Application*		elasticloadbalancing:DeleteListener elasticloadbalancing:DeleteTargetGroup
DeleteEnvironment	Gewährt die Berechtigung zum Löschen einer Laufzeitumgebung	Schreiben	Environment*		elasticloadbalancing:DeleteLoadBalancer
GetApplication	Gewährt die Berechtigung zum Abrufen aller Anwendung	Lesen	Application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetApplicationVersion	Gewährt die Berechtigung zum Abrufen einer Anwendungsversion	Lesen	Application*		
GetBatchJobExecution	Gewährt die Berechtigung zum Abrufen einer Batch-Auftragsausführung	Lesen	Application*		
GetDataSetDetails	Gewährt die Berechtigung zum Abrufen von Details eines Datensatzes	Lesen	Application*		
GetDataSetImportTask	Gewährt die Berechtigung zum Abrufen einer Datensatzimportaufgabe	Lesen	Application*		
GetDeployment	Gewährt die Berechtigung zum Abrufen einer Bereitstellung	Lesen	Application*		
GetEnvironment	Gewährt die Berechtigung zum Abrufen einer Laufzeitumgebung	Lesen	Environment*		
GetSignedBluinsightsUrl	Erteilt die Berechtigung, eine signierte Bluinsights-URL zu erstellen	Lesen			
ListApplicationVersions	Gewährt die Berechtigung zum Auflisten der Versionen der Anwendung	Lesen	Application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListApplications	Gewährt die Berechtigung zum Auflisten von Anwendungen	Auflisten			
ListBatchJobDefinitions	Gewährt die Berechtigung zum Auflisten von Batch-Jobdefinitionen	Lesen	Application*		
ListBatchJobExecutions	Gewährt die Berechtigung zum Auflisten von Batch-Jobausführungen	Lesen	Application*		
ListBatchJobRestartPoints	Gewährt die Berechtigung zum Abrufen einer Batch-Auftragsausführung	Lesen	Application*		
ListDataSetImportHistory	Gewährt die Berechtigung zum Auflisten von Datensatz-Importhistorie	Lesen	Application*		
ListDataSets	Gewährt die Berechtigung zum Auflisten von Datensätzen	Lesen	Application*		
ListDeployments	Gewährt die Berechtigung zum Auflisten von Bereitstellungen	Lesen	Application*		
ListEngineVersions	Gewährt die Berechtigung zum Auflisten von Motorvarianten	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListEnvironments	Gewährt die Berechtigung zum Auflisten von Laufzeitumgebungen	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen			
StartApplication	Gewährt die Berechtigung zum Starten einer Anwendung	Schreiben	Application*		
StartBatchJob	Gewährt die Berechtigung zum Starten eines Batch-Jobs	Schreiben	Application*		
StopApplication	Gewährt die Berechtigung zum Beenden einer Anwendung	Schreiben	Application*		
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren	Application		
			Environment		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Markieren	Application		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			Environment		
				aws:TagKeys	
UpdateApplication	Gewährt die Berechtigung zum Aktualisieren einer Anwendung	Schreiben	Application*		s3:GetObject s3:ListBucket
UpdateEnvironment	Gewährt die Berechtigung zum Aktualisieren einer Laufzeitumgebung	Schreiben	Environment*		

Von AWS -Mainframe-Modernisierungsservice definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Application	`arn:${Partition}:m2:${Region}:${Account}:app/${ApplicationId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
Environment	`arn:${Partition}:m2:${Region}:${Account}:env/${EnvironmentId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS -Mainframe-Modernisierungsservice

AWS Der Mainframe Modernization Service definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wertepaaren, die in der Anforderung zulässig sind	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paar einer Ressource	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach Liste von Tag-Schlüsseln, die in der Anforderung zulässig sind	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Managed Blockchain

Amazon Managed Blockchain (Servicepräfix: `managedblockchain`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Managed Blockchain definierte Aktionen
- Von Amazon Managed Blockchain definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Managed Blockchain

Von Amazon Managed Blockchain definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAccessor	Gewährt die Berechtigung zum Erstellen eines Amazon Managed Blockchain-Netzwerks	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	
CreateMember	Gewährt die Berechtigung zum Erstellen eines Mitglieds eines Amazon Managed Blockchain-Netzwerks	Write	network*		iam:CreateServiceLinkedRole
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateNetwork	Gewährt die Berechtigung zum Erstellen eines Amazon Managed Blockchain-Netzwerks	Write		aws:TagKeys	iam:CreateServiceLinkedRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey}	
CreateNode	Gewährt die Berechtigung zum Erstellen eines Knotens innerhalb eines Mitglieds eines Amazon Managed Blockchain-Netzwerks	Write	member		iam:CreateServiceLinkedRole
			network		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateProposal	Gewährt die Berechtigung zum Erstellen eines Vorschlags, dass andere Mitglieder des Blockchain-Netzwerks darüber abstimmen können, ob ein Mitglied in einem Amazon Managed Blockchain-Netzwerk hinzugefügt oder entfernt werden soll	Schreiben	network*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteAccessor	Gewährt die Berechtigung zum Erstellen eines Amazon Managed Blockchain-Netzwerks	Schreiben	accessor*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteMember	Gewährt die Berechtigung zum Löschen eines Mitglieds und aller zugehörigen Ressourcen aus einem Amazon Managed Blockchain-Netzwerk	Write	member*		
DeleteNode	Gewährt die Berechtigung zum Löschen eines Knotens von einem Mitglied eines Amazon Managed Blockchain-Netzwerks	Schreiben	node*		
GET [nur Berechtigung]	Gewährt die Berechtigung zum Senden von HTTP GET-Anforderungen an einen Ethereum-Knoten	Berechtigungsverwaltung			
GetAccessor	Gewährt die Berechtigung zur Rückgabe detaillierter Informationen über ein Amazon Managed Blockchain-Netzwerk	Lesen	accessor*		
GetMember	Gewährt die Berechtigung zur Rückgabe detaillierter Informationen zu einem Mitglied eines Amazon Managed Blockchain-Netzwerks	Read	member*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetNetwork	Gewährt die Berechtigung zur Rückgabe detaillierter Informationen über ein Amazon Managed Blockchain-Netzwerk	Read	network*		
GetNode	Gewährt die Berechtigung zur Rückgabe detaillierter Informationen über einen Knoten innerhalb eines Mitglieds eines Amazon Managed Blockchain-Netzwerks	Read	node*		
GetProposal	Gewährt die Berechtigung zur Rückgabe detaillierter Informationen über einen Vorschlag eines Amazon Managed Blockchain-Netzwerks	Lesen	proposal*		
Invoke [nur Berechtigung]	Erteilt die Erlaubnis, WebSocket-Verbindungen zu einem Ethereum-Knoten herzustellen	Berechtigungsverwaltung			
InvokeRpcBitcoinMainnet	Gewährt die Berechtigung, die Bitcoin-Mainnet-RPCs aufzurufen	Lesen			
InvokeRpcBitcoinTestnet	Gewährt die Berechtigung, die Bitcoin-Testnet-RPCs aufzurufen	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
InvokeRpcPolygonMainnet	Gewährt die Berechtigung, die Polygon-Mainnet-RPCs aufzurufen	Lesen			
InvokeRpcPolygonMumbaiTestnet	Gewährt die Berechtigung, die Polygon-Mumbai-Testnet-RPCs aufzurufen	Lesen			
ListAccessors	Gewährt die Berechtigung zum Auflisten der Amazon-Managed-Blockchain-Netzwerke, die sich im aktuellen teilnimmt AWS-Konto	Auflisten			
ListInvitations	Gewährt die Berechtigung zum Auflisten der Einladungen, die auf das aktive AWS-Konto von einem Managed-Blockchain-Netzwerk erweitert wurden	List			
ListMembers	Gewährt die Berechtigung zum Auflisten der Mitglieder eines Amazon Managed Blockchain-Netzwerks und der Eigenschaften ihrer Mitgliedschaften	List	network*		
ListNetworks	Gewährt die Erlaubnis, die Amazon-Managed-Blockchain-Netzwerke aufzulisten, an denen das aktuelle AWS-Konto teilnimmt	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListNodes	Gewährt die Berechtigung zum Auflisten der Knoten innerhalb eines Mitglieds eines Amazon Managed Blockchain-Netzwerks	List	member		
			network		
ListProposalVotes	Gewährt die Berechtigung zum Auflisten aller Stimmen für einen Vorschlag, einschließlich des Werts der Abstimmung und der eindeutigen Kennung des Mitglieds, das die Stimme für das angegebene Amazon Managed Blockchain-Netzwerk abgegeben hat	Read	proposal*		
ListProposals	Gewährt die Berechtigung zum Auflisten von Vorschlägen für das angegebene Amazon Managed Blockchain-Netzwerk	List	network*		
ListTagsForResource	Gewährt die Berechtigung zum Anzeigen von Tags, die mit einer Amazon Managed Blockchain-Ressource verknüpft sind	Lesen	accessor		
			invitation		
			member		
			network		
			node		
			proposal		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
POST [nur Berechtigung]	Gewährt die Berechtigung zum Senden von HTTP POST-Anforderungen an einen Ethereum-Knoten	Berechtigungsverwaltung			
RejectInvitation	Gewährt die Berechtigung zum Ablehnen der Einladung zur Teilnahme am Blockchain-Netzwerk	Write	invitation*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Amazon Managed Blockchain-Ressource	Markieren	accessor		
			invitation		
			member		
			network		
			node		
			proposal		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Amazon Managed Blockchain-Ressource	Markieren	accessor		
			invitation		
			member		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			network		
			node		
			proposal		
				aws:TagKeys	
UpdateMember	Gewährt die Berechtigung zum Erstellen eines Mitglieds eines Amazon Managed Blockchain-Netzwerks.	Write	member*		iam:CreateServiceLinkedRole
UpdateNode	Gewährt die Berechtigung zum Aktualisieren eines Knotens von einem Mitglied eines Amazon Managed Blockchain-Netzwerks.	Write	node*		iam:CreateServiceLinkedRole
VoteOnProposal	Gewährt die Berechtigung zum Abgeben einer Stimme für einen Vorschlag im Namen des angegebenen Mitglieds des Blockchain-Netzwerks	Write	proposal*		

Von Amazon Managed Blockchain definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
network	`arn:${Partition}:managedblockchain:${Region}::networks/${NetworkId}`	aws:ResourceTag/${TagKey}
member	`arn:${Partition}:managedblockchain:${Region}:${Account}:members/${MemberId}`	aws:ResourceTag/${TagKey}
node	`arn:${Partition}:managedblockchain:${Region}:${Account}:nodes/${NodeId}`	aws:ResourceTag/${TagKey}
proposal	`arn:${Partition}:managedblockchain:${Region}::proposals/${ProposalId}`	aws:ResourceTag/${TagKey}
invitation	`arn:${Partition}:managedblockchain:${Region}:${Account}:invitations/${InvitationId}`	aws:ResourceTag/${TagKey}
accessor	`arn:${Partition}:managedblockchain:${Region}:${Account}:accessors/${AccessorId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Managed Blockchain

Amazon Managed Blockchain definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf den Markierungen, die in der Anforderung übergeben werden.	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf den Tags, die mit einer Amazon Managed Blockchain-Ressource verknüpft sind	Zeichenfolge
aws:TagKeys	Filtert Aktionen basierend auf den Tag-Schlüsseln, die in der Anforderung übergeben werden.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Managed Blockchain Query

Amazon Managed Blockchain Query (Servicepräfix: `managedblockchain-query`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Managed Blockchain Query definierte Aktionen
- Von Amazon Managed Blockchain Query definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Managed Blockchain Query

Von Amazon Managed Blockchain Query definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetTokenBalance	Gewährt die Berechtigung zum Stapeln von Aufrufen für die GetTokenBalance API	Lesen			
GetAssetContract	Gewährt die Berechtigung zum Abrufen von Informationen über einen Vertrag in der Blockchain	Lesen			
GetTokenBalance	Gewährt die Berechtigung zum Abrufen des Saldos eines Tokens für eine Adresse in der Blockchain	Lesen			
GetTransaction	Gewährt die Berechtigung zum Abrufen einer Transaktion in der Blockchain	Lesen			
ListAssetContracts	Gewährt die Berechtigung zum Abrufen mehrerer Verträge in der Blockchain	Auflisten			
ListFilteredTransactionEvents	Gewährt die Berechtigung zum Abrufen von Ereignissen in der Blockchain mit zusätzlichen Filtern	Auflisten			
ListTokenBalances	Gewährt die Berechtigung zum Abrufen mehrerer Salden einer Transaktion in der Blockchain	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTransactionEvents	Gewährt die Berechtigung zum Abrufen von Ereignissen einer Transaktion in der Blockchain	Auflisten			
ListTransactions	Gewährt die Berechtigung zum Abrufen mehrerer Transaktionen in der Blockchain	Auflisten			

Von Amazon Managed Blockchain Query definierte Ressourcentypen

Amazon Managed Blockchain Query unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf Amazon Managed Blockchain Query zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für Amazon Managed Blockchain Query

Amazon Managed Blockchain Query besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Managed Grafana

Amazon Managed Grafana (Servicepräfix: `grafana`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.

- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Managed Grafana definierte Aktionen
- Von Amazon Managed Grafana definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Managed Grafana

Von Amazon Managed Grafana definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Associate License	Gewährt die Berechtigung zum Upgrade eines Workspace mit einer Lizenz	Write	workspace*		aws-marketplace:ViewSubscriptions
CreateWorkspace	Gewährt die Berechtigung zum Erstellen eines Workspace	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetManagedPrefixListEntries iam:CreateServiceLinkedRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					organizations:DescribeOrganization sso:CreateManagedApplicationInstance sso:DescribeRegisteredRegions sso:GetSharedSsoConfiguration
CreateWorkspaceApiKey	Erteilt die Berechtigung zum Erstellen von API-Schlüsseln für einen Arbeitsbereich	Schreiben	workspace*		
CreateWorkspaceServiceAccount	Erteilt die Berechtigung zum Erstellen von Dienstkonten für einen Workspace	Schreiben	workspace*		
CreateWorkspaceServiceAccountToken	Erteilt die Berechtigung zum Erstellen von Dienstkonto-Tokens für einen Workspace	Schreiben	workspace*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteWorkspace	Gewährt die Berechtigung zum Löschen eines Workspace	Schreiben	workspace*		sso:DeleteManagedApplicationInstance
DeleteWorkspaceApiKey	Erteilt die Berechtigung zum Löschen von API-Schlüsseln aus einem Workspace	Schreiben	workspace*		
DeleteWorkspaceServiceAccount	Erteilt die Berechtigung zum Löschen von Dienstkonten für einen Workspace	Schreiben	workspace*		
DeleteWorkspaceServiceAccountToken	Erteilt die Berechtigung zum Löschen von Dienstkonto-Tokens für einen Workspace	Schreiben	workspace*		
DescribeWorkspace	Gewährt die Berechtigung zum Beschreiben eines Workspace	Lesen	workspace*		
DescribeWorkspaceAuthentication	Gewährt die Berechtigung zum Beschreiben von Authentifizierungsanbietern in einem Workspace	Lesen	workspace*		
DescribeWorkspaceConfiguration	Gewährt die Berechtigung zum Beschreiben der aktuellen Konfigurationszeichenfolge für den angegebenen Workspace	Lesen	workspace*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateLicense	Gewährt die Berechtigung zum Entfernen einer Lizenz aus einer Workspace	Write	workspace*		
ListPermissions	Gewährt die Berechtigung zum Auflisten der Berechtigungen für einen Workspace	Auflisten	workspace*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags, die mit einem Workspace verknüpft sind	Lesen	workspace		
ListVersions	Gewährt die Berechtigung zum Auflisten aller verfügbaren unterstützten Grafana-Versionen Fügen Sie optional einen Arbeitsbereich hinzu, in dem die Versionen aufgeführt sind, auf die ein Upgrade möglich ist.	Auflisten	workspace		
ListWorkspaceServiceAccountTokens	Erteilt die Berechtigung, Dienstkonto-Token für einen Workspace aufzulisten	Lesen	workspace*		
ListWorkspaceServiceAccounts	Erteilt die Berechtigung, Dienstkonten für einen Workspace aufzulisten	Lesen	workspace*		
ListWorkspaces	Gewährt die Berechtigung zum Auflisten von Workspaces	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu oder zum Aktualisieren von Tagwerten eines Workspace	Tagging	workspace*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einem Workspace	Tagging	workspace*		
				aws:TagKeys	
UpdatePermissions	Gewährt die Berechtigung zum Ändern der Berechtigungen für einen Workspace	Berechtigungsverwaltung	workspace*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateWorkspace	Gewährt die Berechtigung zum Ändern eines Workspace	Schreiben	workspace*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetManagedPrefixListEntries iam:CreateServiceLinkedRole
UpdateWorkspaceAuthentication	Gewährt die Berechtigung zum Ändern von Authentifizierungsanbietern in einem Workspace	Schreiben	workspace*		
UpdateWorkspaceConfiguration	Gewährt die Berechtigung zum Aktualisieren der Konfiguration zum Aktualisieren der Konfiguration	Schreiben	workspace*		

Von Amazon Managed Grafana definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
workspace	`arn:${Partition}:grafana:${Region}:${Account}:/workspaces/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Managed Grafana

Amazon Managed Grafana definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff danach, ob Tag-Schlüssel-Wert-Paare in der Anforderung vorhanden sind	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tag-Schlüssel-Wert-Paaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert Zugriff basierend auf dem Vorhandensein von Tag-Schlüsseln in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Managed Service for Prometheus

Amazon Managed Service for Prometheus (Servicepräfix: `aps`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Managed Service for Prometheus definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAlertManagerAlerts	Gewährt die Berechtigung zum Erstellen von Alarmen	Schreiben	workspace*		
				aws:ResourceTag/${TagKey}	
CreateAlertManagerDefinition	Gewährt die Berechtigung zum Erstellen einer Warnmanager-Definition	Schreiben	workspace*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateLoggingConfiguration	Gewährt die Berechtigung zum Erstellen einer Protokollierungskonfiguration.	Schreiben	workspace*		
				aws:ResourceTag/${TagKey}	
CreateRuleGroupsNamespace	Gewährt die Berechtigung zum Erstellen eines Regelgruppen-Namespace	Schreiben	rulegroupsnamespace*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateScraper	Gewährt die Berechtigung zum Erstellen eines Scrapers	Schreiben	cluster*		aps:TagResource ec2:DescribeSecurityGroups ec2:DescribeSubnets eks:DescribeCluster iam:CreateServiceLinkedRole
			workspace*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateWorkspace	Gewährt die Berechtigung zum Erstellen eines Workspace	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAlertManagerDefinition	Gewährt die Berechtigung zum Löschen einer Warnmanager-Definition	Schreiben	workspace*		
				aws:ResourceTag/${TagKey}	
DeleteAlertManagerSilence	Gewährt die Berechtigung zum Löschen einer Silence	Schreiben	workspace*		
				aws:ResourceTag/${TagKey}	
DeleteLoggingConfiguration	Gewährt die Berechtigung zum Löschen einer Protokollierungskonfiguration.	Schreiben	workspace*		
				aws:ResourceTag/${TagKey}	
DeleteRuleGroupsNamespace	Gewährt die Berechtigung zum Löschen eines Regelgruppen-Namespace	Schreiben	rulegroupsnamespace*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
DeleteScraper	Gewährt die Berechtigung zum Löschen eines Scrapers	Schreiben	scraper*		
				aws:ResourceTag/${TagKey}	
DeleteWorkspace	Gewährt die Berechtigung zum Löschen eines Workspace	Schreiben	workspace*		
				aws:ResourceTag/${TagKey}	
DescribeAlertManagerDefinition	Gewährt die Berechtigung zum Beschreiben einer Warnmanager-Definition	Lesen	workspace*		
				aws:ResourceTag/${TagKey}	
DescribeLoggingConfiguration	Gewährt die Berechtigung zum Beschreiben einer Protokollierungskonfiguration.	Lesen	workspace*		
				aws:ResourceTag/${TagKey}	
DescribeRuleGroupsNamespace	Gewährt die Berechtigung zum Beschreiben eines Regelgruppen-Namespace	Lesen	rulegroupsnamespace*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
DescribeScraper	Gewährt die Berechtigung zum Beschreiben eines Scrapers	Lesen	scraper*		
				aws:ResourceTag/${TagKey}	
DescribeWorkspace	Gewährt die Berechtigung zum Beschreiben eines Workspace	Lesen	workspace*		
				aws:ResourceTag/${TagKey}	
GetAlertManagerSilence	Gewährt die Berechtigung zum Erhalten einer Silence	Lesen	workspace*		
				aws:ResourceTag/${TagKey}	
GetAlertManagerStatus	Gewährt die Berechtigung zum Erhalten des aktuellen Status eines Warnmanagers	Lesen	workspace*		
				aws:ResourceTag/${TagKey}	
GetDefaultScraperConfiguration	Gewährt die Berechtigung zum Abrufen einer Standard-Scraper-Konfiguration	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetLabels	Gewährt die Berechtigung zum Abrufen von AMP Workspace-Bezeichnungen	Read	workspace*		
				aws:ResourceTag/${TagKey}	
GetMetricMetadata	Gewährt die Berechtigung zum Abrufen der Metadaten für AMP Workspace-Metriken	Read	workspace*		
				aws:ResourceTag/${TagKey}	
GetSeries	Gewährt die Berechtigung zum Abrufen von AMP Workspace-Zeitreihendaten	Lesen	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlertManagerAlertGroups	Gewährt die Berechtigung zum Auflisten von Gruppen	Lesen	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlertManagerAlerts	Gewährt die Berechtigung zum Auflisten von Alarmen	Lesen	workspace*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAlertManagerReceivers	Gewährt die Berechtigung zum Auflisten von Receivern	Lesen	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlertManagerSilences	Gewährt die Berechtigung zum Auflisten von Silences	Lesen	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlerts	Gewährt die Berechtigung zum Auflisten von aktiven Warnungen	Lesen	workspace*		
				aws:ResourceTag/${TagKey}	
ListRuleGroupsNamespaces	Gewährt die Berechtigung zum Auflisten von Regelgruppen-Namespaces	Auflisten	workspace*		
				aws:ResourceTag/${TagKey}	
ListRules	Gewährt die Berechtigung zum Auflisten von Warnungen und Aufzeichnungsregeln	Lesen	workspace*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListScrapers	Gewährt die Berechtigung zum Auflisten von Scrapern	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags in einer AMP-Ressource	Lesen	rulegroupsnamespace		
			scraper		
			workspace		
				aws:TagKeys aws:RequestTag/${TagKey}	
ListWorkspaces	Gewährt die Berechtigung zum Auflisten von Workspaces	Auflisten			
PutAlertManagerDefinition	Gewährt die Berechtigung zum Aktualisieren einer Warnmanager-Definition	Schreiben	workspace*		
				aws:ResourceTag/${TagKey}	
PutAlertManagerSilences	Gewährt die Berechtigung zum Erstellen oder Aktualisieren einer Silence	Schreiben	workspace*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutRuleGroupsNamespace	Gewährt die Berechtigung zum Aktualisieren eines Regelgruppen-Namespace	Schreiben	rulegroupsnamespace*		
				aws:ResourceTag/${TagKey}	
QueryMetrics	Gewährt die Berechtigung zum Ausführen einer Abfrage für AMP Workspace-Metriken	Read	workspace*		
				aws:ResourceTag/${TagKey}	
RemoteWrite	Gewährt die Berechtigung zum Durchführen eines Remote-Schreibvorgangs, um das Streaming von Metriken an AMP Workspace zu initiieren	Schreiben	workspace*		
				aws:ResourceTag/${TagKey}	
TagResource	Gewährt die Berechtigung zum Markieren einer AMP-Ressource	Markierung	rulegroupsnamespace		
			scraper		
			workspace		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer AMP-Ressource	Markierung	rulegroupsnamespace		
			scraper		
			workspace		
				aws:TagKeys	
UpdateLoggingConfiguration	Gewährt die Berechtigung zum Aktualisieren einer Protokollierungskonfiguration.	Schreiben	workspace*		
				aws:ResourceTag/${TagKey}	
UpdateWorkspaceAlias	Gewährt die Berechtigung zum Ändern des Alias des bestehenden AMP-Workspace	Write	workspace*		
				aws:ResourceTag/${TagKey}	

Von Amazon Managed Service for Prometheus definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
workspace	`arn:${Partition}:aps:${Region}:${Account}:workspace/${WorkspaceId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
rulegroupsnamespace	`arn:${Partition}:aps:${Region}:${Account}:rulegroupsnamespace/${WorkspaceId}/${Namespace}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
scraper	`arn:${Partition}:aps:${Region}:${Account}:scraper/${ScraperId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
cluster	`arn:${Partition}:eks:${Region}:${Account}:cluster/${ClusterName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Managed Service for Prometheus

Amazon Managed Service für Prometheus definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüsseln, die in der Anforderung übergeben werden.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Managed Streaming for Apache Kafka

Amazon Managed Streaming for Apache Kafka (Servicepräfix: `kafka`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Managed Streaming for Apache Kafka definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchAssociateScramSecret	Gewährt die Berechtigung, einen oder mehrere Scram Secrets einem Amazon MSK-Cluster zuzuordnen	Write	cluster*		kms:CreateGrant kms:RetireGrant
BatchDisassociateScramSecret	Gewährt die Berechtigung, die Mapping eines oder mehrerer Scram Secrets zu einem Amazon MSK-Cluster aufzuheben	Write	cluster*		kms:RetireGrant
CreateCluster	Gewährt die Berechtigung zum Erstellen eines MSK-Clusters	Schreiben	cluster*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:AttachRolePolicy

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					iam:CreateServiceLinkedRole iam:PutRolePolicy kms:CreateGrant kms:DescribeKey
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateClusterV2	Gewährt die Berechtigung zum Erstellen eines MSK-Clusters	Write	cluster*		ec2:CreateTags ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs iam:AttachRolePolicy

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					iam:CreateServiceLinkedRole iam:PutRolePolicy kms:CreateGrant kms:DescribeKey
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfiguration	Gewährt die Berechtigung zum Erstellen einer MSK-Konfiguration	Schreiben	configuration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateReplicator	Gewährt die Berechtigung zum Erstellen eines MSK-Replikators	Schreiben	replicator*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PassRole iam:PutRolePolicy kafka:DescribeClusterV2 kafka:GetBootstrapBrokers

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateVpcConnection	Gewährt die Berechtigung zum Erstellen einer MSK-VPC-Verbindung	Schreiben	cluster*		ec2:CreateTags ec2:CreateVpcEndpoint ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs iam:AttachRolePolicy iam:CreateServiceLinkedRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					iam:PutRolePolicy
			vpc-connection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCluster	Gewährt die Berechtigung zum Löschen eines MSK-Clusters	Schreiben	cluster*		ec2:DeleteVpcEndpoints ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints
DeleteClusterPolicy	Gewährt die Berechtigung zum Löschen einer auf Cluster-Ressourcen basierenden Richtlinie	Schreiben	cluster*		
DeleteConfiguration	Gewährt die Berechtigung zum Löschen der angegebenen MSK-Konfiguration	Schreiben	configuration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteReplicator	Gewährt die Berechtigung zum Löschen eines MSK-Replikators	Schreiben	replicator*		
DeleteVpcConnection	Gewährt die Berechtigung zum Löschen einer MSK-VPC-Verbindung	Schreiben	vpc-connection*		ec2:DeleteVpcEndpoints ec2:DescribeVpcEndpoints
DescribeCluster	Gewährt die Berechtigung zum Beschreiben eines MSK-Clusters	Read	cluster*		
DescribeClusterOperation	Gewährt die Berechtigung zum Beschreiben des Clustervorgangs, der durch den entsprechenden ARN angegeben wird	Lesen			
DescribeClusterOperationV2	Gewährt die Berechtigung zum Beschreiben des Clustervorgangs, der durch den entsprechenden ARN angegeben wird	Lesen			
DescribeClusterV2	Gewährt die Berechtigung zum Beschreiben eines MSK-Clusters	Lesen	cluster*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeConfiguration	Gewährt die Berechtigung zum Beschreiben einer MSK-Konfiguration	Read	configuration*		
DescribeConfigurationRevision	Gewährt die Berechtigung zum Beschreiben einer MSK-Konfigurationsrevision	Lesen	configuration*		
DescribeReplicator	Gewährt die Berechtigung zum Beschreiben eines MSK-Replikators	Lesen	replicator*		
DescribeVpcConnection	Gewährt die Berechtigung zum Beschreiben einer MSK-VPC-Verbindung	Lesen	vpc-connection*		
GetBootstrapBrokers	Gewährt die Berechtigung zum Abrufen von Verbindungsdetails für die Broker in einem MSK-Cluster	Lesen			
GetClusterPolicy	Gewährt die Berechtigung zum Beschreiben einer auf Cluster-Ressourcen basierenden Richtlinie	Lesen	cluster*		
GetCompatibleKafkaVersions	Gewährt die Berechtigung zum Abrufen einer Liste der Apache Kafka-Versionen, auf die Sie einen MSK-Cluster aktualisieren können	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListClientVpcConnections	Gewährt die Berechtigung zum Auflisten aller MSK-VPC-Verbindungen, die für einen Cluster erstellt wurden	Auflisten	cluster*		
ListClusterOperations	Gewährt die Berechtigung, eine Liste aller Vorgänge zurückzugeben, die im angegebenen MSK-Cluster ausgeführt wurden	Auflisten	cluster*		
ListClusterOperationsV2	Gewährt die Berechtigung, eine Liste aller Vorgänge zurückzugeben, die im angegebenen MSK-Cluster ausgeführt wurden	List	cluster*		
ListClusters	Gewährt die Berechtigung zum Auflisten aller MSK-Cluster in diesem Konto	Auflisten			
ListClustersV2	Gewährt die Berechtigung zum Auflisten aller MSK-Cluster in diesem Konto	List			
ListConfigurationRevisions	Gewährt die Berechtigung zum Auflisten aller Revisionen für eine MSK-Konfiguration in diesem Konto	List	configuration*		
ListConfigurations	Gewährt die Berechtigung zum Auflisten aller MSK-Konfigurationen in diesem Konto	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListKafkaVersions	Gewährt die Berechtigung zum Auflisten aller von Amazon MSK unterstützten Apache Kafka-Versionen	List			
ListNodes	Gewährt die Berechtigung zum Auflisten der Broker in einem MSK-Cluster	Auflisten	cluster*		
ListReplicators	Gewährt die Berechtigung zum Auflisten aller MSK-Replikatoren in diesem Konto	Auflisten			
ListScramSecrets	Gewährt die Berechtigung zum Auflisten der Scram Secrets, die einem Amazon MSK-Cluster zugeordnet sind	List	cluster*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags einer MSK-Ressource	Lesen	cluster*		
ListVpcConnections	Gewährt die Berechtigung zum Auflisten aller MSK-VPC-Verbindungen, die in diesem Konto verwendet werden	Auflisten			
PutClusterPolicy	Gewährt die Berechtigung zum Erstellen oder Aktualisieren der ressourcenbasierten Richtlinie für einen Cluster	Schreiben	cluster*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RebootBroker	Gewährt die Berechtigung, einen Broker neu zu starten	Schreiben	cluster*		
RejectClientVpcConnection	Gewährt die Berechtigung zum Ablehnen einer MSK-VPC-Verbindung	Schreiben	cluster*		
			vpc-connection*		
TagResource	Gewährt die Berechtigung zum Markieren einer MSK-Ressource	Markieren	cluster		
			vpc-connection		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer MSK-Ressource	Markieren	cluster		
			vpc-connection		
				aws:TagKeys	
UpdateBrokerCount	Gewährt die Berechtigung, die Anzahl der Broker des MSK-Clusters zu aktualisieren	Write	cluster*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateBrokerStorage	Gewährt die Berechtigung, die Speichergröße der Broker des MSK-Clusters zu aktualisieren	Write	cluster*		
UpdateBrokerType	Gewährt die Berechtigung zur Aktualisierung des Brokertyps eines Amazon MSK-Clusters	Write	cluster*		
UpdateClusterConfiguration	Gewährt die Berechtigung zum Aktualisieren der Konfiguration des MSK-Clusters	Write	cluster* configuration*		
UpdateClusterKafkaVersion	Gewährt die Berechtigung zum Aktualisieren des MSK-Clusters auf die angegebene Apache Kafka-Version	Write	cluster*		
UpdateConfiguration	Gewährt die Berechtigung zum Erstellen einer neuen Revision der MSK-Konfiguration	Schreiben	configuration*		
UpdateConnectivity	Gewährt die Berechtigung zum Aktualisieren der Konnektivitäts-Einstellungen für den MSK-Cluster	Schreiben	cluster*		ec2:DescribeRouteTables ec2:DescribeSubnets

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				kafka:publicAccessEnabled	
UpdateMonitoring	Gewährt die Berechtigung zum Aktualisieren der Überwachungseinstellungen für den MSK-Cluster	Schreiben	cluster*		
UpdateReplicationInfo	Gewährt die Berechtigung zum Aktualisieren der Replikationsinformationen des MSK-Replikators	Schreiben	replicator*		
UpdateSecurity	Gewährt die Berechtigung zum Aktualisieren der Sicherheitseinstellungen für den MSK-Cluster	Schreiben	cluster*		kms:RetireGrant
UpdateStorage	Gewährt die Berechtigung, den EBS-Speicher (Größe oder bereitgestellter Durchsatz) zu aktualisieren, der MSK-Brokern zugeordnet ist, oder den Cluster-Speichermodus auf TIERED festzulegen	Schreiben	cluster*		

Von Amazon Managed Streaming for Apache Kafka definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden

können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
cluster	`arn:${Partition}:kafka:${Region}:${Account}:cluster/${ClusterName}/${Uuid}`	aws:ResourceTag/${TagKey}
configuration	`arn:${Partition}:kafka:${Region}:${Account}:configuration/${ConfigurationName}/${Uuid}`	
vpc-connection	`arn:${Partition}:kafka:${Region}:${VpcOwnerAccount}:vpc-connection/${ClusterOwnerAccount}/${ClusterName}/${Uuid}`	aws:ResourceTag/${TagKey}
replicator	`arn:${Partition}:kafka:${Region}:${Account}:replicator/${ReplicatorName}/${Uuid}`	aws:ResourceTag/${TagKey}
topic	`arn:${Partition}:kafka:${Region}:${Account}:topic/${ClusterName}/${ClusterUuid}/${TopicName}`	
group	`arn:${Partition}:kafka:${Region}:${Account}:group/${ClusterName}/${ClusterUuid}/${GroupName}`	
transactional-id	`arn:${Partition}:kafka:${Region}:${Account}:transactional-id/${ClusterName}/${ClusterUuid}/${TransactionalId}`	

Bedingungsschlüssel für Amazon Managed Streaming for Apache Kafka

Amazon Managed Streaming for Apache Kafka definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString
kafka:publicAccessEnabled	Filtert den Zugriff danach, ob die Anforderung für den öffentlichen Zugriff freigegeben ist	Bool

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Managed Streaming for Kafka Connect

Amazon Managed Streaming for Kafka Connect (Service-Präfix: `kafkaconnect`) bietet die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.

- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Managed Streaming for Kafka Connect definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWSzu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateConnector	Gewährt die Berechtigung zum Erstellen eines MSK-Connect-Anschlusses	Schreiben			ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs firehose:TagDeliveryStream iam:AttachRolePolicy

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					iam:CreateServiceLinkedRole iam:PassRole iam:PutRolePolicy logs:CreateLogDelivery logs:DescribeLogGroups logs:DescribeResourcePolicies logs:GetLogDelivery logs:ListLogDeliveries logs:PutResourcePolicy

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					s3:GetBucketPolicy s3:PutBucketPolicy
CreateCustomPlugin	Gewährt die Berechtigung zum Erstellen eines benutzerdefinierten MSK-Connect-Plugins	Schreiben			s3:GetObject
CreateWorkerConfiguration	Gewährt die Berechtigung zum Erstellen einer MSK-Connect-Worker-Konfiguration	Schreiben			
DeleteConnector	Gewährt die Berechtigung zum Löschen eines MSK-Connect-Anschlusses	Schreiben	connector*		logs:DeleteLogDelivery logs:ListLogDeliveries
DeleteCustomPlugin	Gewährt die Berechtigung zum Löschen eines benutzerdefinierten MSK-Connect-Plugins	Schreiben	customplugin*		
DeleteWorkerConfiguration	Gewährt die Berechtigung zum Löschen einer MSK-Connect-Worker-Konfiguration	Schreiben	workerconfiguration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeConnector	Gewährt die Berechtigung zum Beschreiben eines MSK-Connect-Anschlusses	Lesen	connector*		
DescribeCustomPlugin	Gewährt die Berechtigung zum Beschreiben eines benutzerdefinierten MSK-Connect-Plugins	Lesen	customplugin*		
DescribeWorkerConfiguration	Gewährt die Berechtigung zum Beschreiben einer MSK-Connect-Worker-Konfiguration	Lesen	workerconfiguration*		
ListConnectors	Gewährt die Berechtigung zum Auflisten aller MSK-Connect-Anschlüsse in diesem Konto	Lesen			
ListCustomPlugins	Gewährt die Berechtigung zum Auflisten aller benutzerdefinierten MSK-Connect-Plugins in diesem Konto	Lesen			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags einer MSK-Connect-Ressource	Lesen	connector	aws:ResourceTag/${TagKey}	
			customplugin	aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			worker configuration	aws:ResourceTag/${TagKey}	
ListWorkerConfigurations	Gewährt die Berechtigung zum Auflisten aller MSK-Connect-Worker-Konfigurationen in diesem Konto	Lesen			
TagResource	Gewährt die Berechtigung zum Markieren einer MSK-Connect-Ressource	Tagging	connector	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			custom plugin	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			worker configuration	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer MSK-Connect-Ressource	Tagging	connector	aws:TagKeys	
			custom plugin	aws:TagKeys	
			worker configuration	aws:TagKeys	
				aws:TagKeys	
UpdateConnector	Gewährt die Berechtigung zum Aktualisieren eines MSK-Connect-Anschlusses	Schreiben	connector *		

Von Amazon Managed Streaming for Kafka Connect definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
connector	`arn:${Partition}:kafkaconnect:${Region}:${Account}:connector/${ConnectorName}/${UUID}`	aws:ResourceTag/${TagKey}
custom plugin	`arn:${Partition}:kafkaconnect:${Region}:${Account}:custom-plugin/${CustomPluginName}/${UUID}`	aws:ResourceTag/${TagKey}
worker configuration	`arn:${Partition}:kafkaconnect:${Region}:${Account}:worker-configuration/${WorkerConfigurationName}/${UUID}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Managed Streaming for Kafka Connect

Amazon Managed Streaming for Kafka Connect definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	String
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Managed Workflows for Apache Airflow

Amazon Managed Workflows for Apache Airflow (Servicepräfix: `airflow`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Managed Workflows for Apache Airflow definierte Aktionen
- Von Amazon Managed Workflows for Apache Airflow definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Managed Workflows for Apache Airflow

Von Amazon Managed Workflows for Apache Airflow definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCliToken	Gewährt die Berechtigung zum Erstellen eines kurzlebigen Tokens, mit dem ein Benutzer die Airflow-CLI über einen Endpunkt auf dem Apache Airflow-Webserver aufrufen kann	Write	environment*		
CreateEnvironment	Gewährt die Berechtigung zum Erstellen einer Amazon MWAA-Umgebung	Write	environment*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebLoginToken	Gewährt die Berechtigung zum Erstellen eines kurzlebigen Tokens, mit dem sich ein Benutzer bei der Apache Airflow-Web-Benutzeroberfläche anmelden kann	Write	rbac-role*		
DeleteEnvironment	Gewährt die Berechtigung zum Löschen einer Amazon MWAA-Umgebung	Write	environment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
GetEnvironment	Gewährt die Berechtigung zum Anzeigen von Details zu einer Amazon MWAA-Umgebung	Read	environment*		
				aws:ResourceTag/${TagKey}	
ListEnvironments	Gewährt die Berechtigung zum Auflisten der Amazon MWAA-Umgebungen in Ihrem Konto	List			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Amazon MWAA-Umgebung	Read	environment		
				aws:ResourceTag/${TagKey}	
PublishMetrics	Gewährt die Berechtigung zum Veröffentlichen von Metriken für eine Amazon MWAA-Umgebung	Write	environment*		
TagResource	Gewährt die Berechtigung zum Markieren einer Amazon MWAA-Umgebung	Markieren	environment		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Gewährt die Berechtigung, die Markierung einer Amazon MWAA-Umgebung aufzuheben	Markieren	environment		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateEnvironment	Gewährt die Berechtigung zum Ändern einer Amazon MWAA-Umgebung	Write	environment*		
				aws:ResourceTag/${TagKey}	

Von Amazon Managed Workflows for Apache Airflow definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden

können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
environment	`arn:${Partition}:airflow:${Region}:${Account}:environment/${EnvironmentName}`	
rbac-role	`arn:${Partition}:airflow:${Region}:${Account}:role/${EnvironmentName}/${RoleName}`	

Bedingungsschlüssel für Amazon Managed Workflows for Apache Airflow

Amazon Managed Workflows for Apache Airflow definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert Aktionen nach den Tag-Schlüsseln in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace

AWS Marketplace (Servicepräfix: `aws-marketplace`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Marketplace definierte Aktionen
- Von AWS Marketplace definierte Ressourcentypen
- Bedingungsschlüssel für AWS Marketplace

Von AWS Marketplace definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn

die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptAgreementApprovalRequest	Berechtigt Benutzer, eine eingehende Abonnementanforderung zu genehmigen (für Anbieter, die Produkte bereitstellen, die eine Abonnementverifizierung erfordern).	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptAgreementRequest	Erteilung der Berechtigung an Benutzer, ihre Zustimmungsanfragen zu akzeptieren. Beachten Sie, dass diese Aktion nicht für Marketplace-Käufe gilt.	Schreiben			
CancelAgreement	Erteilung der Berechtigung an Benutzer, ihre Vereinbarungen zu kündigen. Beachten Sie, dass diese Aktion nicht für Marketplace-Käufe gilt.	Schreiben			
CancelAgreementRequest	Berechtigt Benutzer, ausstehende Abonnementanforderungen für Produkte zu stornieren, für die eine Abonnementverifizierung erforderlich ist	Schreiben			
CreateAgreementRequest	Erteilung der Berechtigung an Benutzer, eine Vereinbarungsanfrage zu erstellen. Beachten Sie, dass diese Aktion nicht für Marketplace-Käufe gilt.	Schreiben			
DescribeAgreement	Gewährt Benutzern die Berechtigung, die Metadaten über die Vereinbarung zu beschreiben	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAgreementApprovalRequest	Berechtigt Benutzer, die Details ihrer eingehenden Abonnementanfragen anzuzeigen (für Anbieter, die Produkte anbieten, die eine Überprüfung des Abonnements erfordern).	Lesen			
GetAgreementRequest	Berechtig Benutzer, die Details ihrer Abonnementanforderungen für Datenprodukte anzuzeigen, für die eine Abonnementverifizierung erforderlich ist	Lesen			
GetAgreementTerms	Gewährt Benutzern die Berechtigung zum Abrufen einer Liste von Bedingungen für eine Vereinbarung	Auflisten			
ListAgreementApprovalRequests	Berechtigt Benutzer, ihre eingehenden Abonnementanforderungen aufzulisten (für Anbieter, die Produkte bereitstellen, für die eine Abonnementverifizierung erforderlich ist)	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAgreementRequests	Berechtigt Benutzer, ausstehende Abonnementanforderungen für Produkte aufzulisten, für die eine Abonnementverifizierung erforderlich ist	Auflisten			
ListEntitlementDetails	Gewährt Benutzern die Berechtigung zum Einsehen von Details der mit einer Vereinbarung verbundenen Berechtigungserteilungen. Beachten Sie, dass diese Aktion nicht für Marketplace-Käufe gilt.	Lesen			
RejectAgreementApprovalRequest	Berechtigt Benutzer, ihre eingehenden Abonnementanforderungen abzulehnen (für Anbieter, die Produkte bereitstellen, für die eine Abonnementverifizierung erforderlich ist)	Schreiben			
SearchAgreements	Gewährt Benutzern die Berechtigung zum Durchsuchen ihrer Vereinbarungen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Subscribe	Gewährt Benutzern die Berechtigung zum Abonnieren von AWS Marketplace-Produkten. Beinhaltet die Möglichkeit, eine Abonnementanfrage für Produkte zu senden, für die eine Abonnementverifizierung erforderlich ist. Beinhaltet die Möglichkeit, die automatische Verlängerung für ein vorhandenes Abonnement zu aktivieren	Schreiben			
Unsubscribe	Gewährt Benutzern die Berechtigung zum Entfernen von Abonnements für AWS Marketplace-Produkte. Beinhaltet die Möglichkeit, die automatische Verlängerung für ein vorhandenes Abonnement zu deaktivieren	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateAgreementApprovalRequest	Berechtigt Benutzer, Änderungen an einer eingehenden Subscription-Anforderung vorzunehmen, einschließlich der Möglichkeit, die Informationen des potenziellen Subscribers zu löschen (für Anbieter, die Produkte bereitstellen, für die eine Abonnementverifizierung erforderlich ist).	Schreiben			
ViewSubscriptions	Gewährt Benutzern die Berechtigung zum Anzeigen der Abonnements ihres Kontos	Auflisten			

Von AWS Marketplace definierte Ressourcentypen

AWS Marketplace unterstützt nicht die Angabe eines Ressourcen-ARN im Element `Resource` einer IAM-Richtlinienanweisung. Um den Zugriff auf AWS Marketplace zuzulassen, geben Sie in Ihrer Richtlinie `"Resource": "*"` an.

Bedingungsschlüssel für AWS Marketplace

AWS Marketplace definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws-marketplace:AgreementType	Filtert den Zugang nach der Art der Vereinbarung	ArrayOfString
aws-marketplace:PartyType	Filtert den Zugang nach der Art der Vereinbarung	Zeichenfolge
aws-marketplace:ProductId	Filtert den Zugriff auf RedHat-OpenShift-Produkte in der AWS Marketplace-RedHat-Konsole nach der Produkt-ID. Hinweis: Dieser Bedingungsschlüssel gilt nur für die RedHat-Konsole, und seine Verwendung schränkt den Zugriff auf Produkte in AWS Marketplace	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace - Katalog

AWS Marketplace Catalog (Dienstpräfix:`aws-marketplace`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Marketplace -Katalog definierte Aktionen
- Von AWS Marketplace -Katalog definierte Ressourcentypen
- Bedingungsschlüssel für AWS Marketplace -Katalog

Von AWS Marketplace -Katalog definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelChangeSet	Gewährt die Berechtigung zum Abbrechen eines laufenden Änderungssatzes	Schreiben	ChangeSet*		
CompleteTask	Gewährt die Berechtigung zum Abschließen einer vorhandenen Aufgabe und zum Senden des Inhalts an die zugeordnete Änderung	Schreiben			
DeleteResourcePolicy	Gewährt die Berechtigung zum Löschen der Ressourcenrichtlinie einer vorhandenen Entität	Berechtigungsverwaltung	Entity*		
DescribeAssessment	Erteilt die Erlaubnis, die Details einer bestehenden Bewertung zurückzugeben	Lesen			
DescribeChangeSet	Gewährt die Berechtigung zum Zurückgeben der Details eines vorhandenen Änderungssatzes	Lesen	ChangeSet*		
DescribeEntity	Gewährt die Berechtigung zum Zurückgeben der Details einer vorhandenen Entität	Lesen	Entity*		
DescribeTask	Gewährt die Berechtigung zum Zurückgeben der Details einer vorhandenen Aufgabe	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetResourcePolicy	Gewährt die Berechtigung zum Abrufen der Ressourcenrichtlinie einer vorhandenen Entität	Lesen	Entity*		
ListAssessments	Erteilt die Erlaubnis, bestehende Bewertungen aufzulisten	Auflisten			
ListChangeSets	Gewährt die Berechtigung zum Auflisten vorhandener Änderungssätze	Auflisten			
ListEntities	Gewährt die Berechtigung zum Auflisten vorhandener Entitäten	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags in einer vorhandenen Entität oder einen Änderungssatz	Lesen	ChangeSet		
			Entity		
ListTasks	Gewährt die Berechtigung zum Auflisten vorhandener Aufgaben	Auflisten			
PutResourcePolicy	Gewährt die Berechtigung zum Hinzufügen einer Ressourcenrichtlinie zu einer vorhandenen Entität	Berechtigungsverwaltung	Entity*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartChangeSet	Erteilt die Berechtigung, einen neuen Änderungssatz anzufordern (Hinweis: Berechtigungen auf Ressourcenebene für diese Aktion und Bedingungskontextschlüssel für diese Aktion werden nur unterstützt, wenn sie mit der Catalog API verwendet werden, und nicht, wenn sie mit dem AWS Marketplace Management Portal verwendet werden)	Schreiben	Entity*		
				catalog:ChangeType aws-marketplace:Intent aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Gewährt die Berechtigung zum Markieren einer bestehenden Entität oder eines Änderungssatzes	Tagging	ChangeSet		
			Entity		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer vorhandenen Entität oder eines Änderungssatzes	Tagging	ChangeSet		
			Entity		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateTask	Gewährt die Berechtigung zum Aktualisieren der Inhalte einer bestehenden Aufgabe	Schreiben			

Von AWS Marketplace -Katalog definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Entity	`arn:${Partition}:aws-marketplace:${Region}:${Account}:${Catalog}/${EntityType}/${ResourceId}`	aws:ResourceTag/${TagKey} catalog:ChangeType
ChangeSet	`arn:${Partition}:aws-marketplace:${Region}:${Account}:${Catalog}/ChangeSet/${ResourceId}`	aws:ResourceTag/${TagKey} catalog:ChangeType

Bedingungsschlüssel für AWS Marketplace -Katalog

AWS Marketplace Catalog definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws-marketplace:Intent	Filtert den Zugriff anhand des Intent-Parameters in der Anfrage StartChangeSet	String
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString
catalog:ChangeType	Filtert den Zugriff nach dem Änderungstyp in der StartChangeSet Anfrage	String

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace Commerce Analytics Service

AWS Marketplace Marketplace Commerce Analytics Service (Servicepräfix: `marketplacecommerceanalytics`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.

Themen

- Von AWS Marketplace Commerce Analytics Service definierte Aktionen
- Von AWS Marketplace Commerce Analytics Service definierte Ressourcentypen
- Bedingungsschlüssel für AWS Marketplace Commerce Analytics Service

Von AWS Marketplace Commerce Analytics Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GenerateDataSet	Fordert die Veröffentlichung eines Dataset in Ihrem Amazon-S3-Bucket an	Write			
StartSupportDataExport	Fordert die Veröffentlichung eines Support-Dataset in Ihrem Amazon-S3-Bucket an	Write			

Von AWS Marketplace Commerce Analytics Service definierte Ressourcentypen

AWS Marketplace Commerce Analytics Service unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf AWS Marketplace Commerce Analytics Service zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Marketplace Commerce Analytics Service

CAS besitzt keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace Deployment Service

AWS Marketplace Deployment Service (Servicepräfix: `aws-marketplace`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.

- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Vom AWS Marketplace Deployment Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Bereitstellungsparameter-Ressource	Lesen	DeploymentParameter		
				aws:ResourceTag/${TagKey}	
PutDeploymentParameter	Gewährt die Berechtigung zum Erstellen oder Aktualisieren einer Bereitstellungsparameter-Ressource	Schreiben	DeploymentParameter*	aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	aws-marketplace:TagResource
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Gewährt die Berechtigung zum Kennzeichnen einer Bereitstellungsparameter-Ressource	Markierung	DeploymentParameter*	aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Bereitstellungsparameter-Ressource	Markierung	DeploymentParameter*	aws:ResourceTag/${TagKey} aws:TagKeys	
				aws:ResourceTag/${TagKey} aws:TagKeys	

Von AWS Marketplace Deployment Service definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
DeploymentParameter	`arn:${Partition}:aws-marketplace:${Region}:${Account}:DeploymentParameter:catalogs/${CatalogName}/products/${ProductId}/${ResourceId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
		aws:TagKeys

Bedingungsschlüssel für AWS Marketplace Deployment Service

AWS Marketplace Deployment Service definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch Tags, die in der Anforderung übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf Tags, die der Ressource zugeordnet sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf Tag-Schlüsseln, die in der Anforderung übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace Discovery

AWS Marketplace Discovery (Servicepräfix: `aws-marketplace`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.

- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Marketplace Discovery definierte Aktionen
- Von AWS Marketplace Discovery definierte Ressourcentypen
- Bedingungsschlüssel für AWS Marketplace Discovery

Von AWS Marketplace Discovery definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListPrivateListings	Gewährt Benutzern die Berechtigung zum Auflisten ihrer privaten Angebote	Auflisten			

Von AWS Marketplace Discovery definierte Ressourcentypen

AWS Marketplace Discovery unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf AWS Marketplace Discovery zuzulassen, geben Sie in Ihrer Richtlinie `"Resource": "*"` an.

Bedingungsschlüssel für AWS Marketplace Discovery

Marketplace Discovery hat keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace Entitlement Service

AWS Marketplace Der Entitlement Service (Dienstpräfix:`aws-marketplace`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Marketplace Entitlement Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetEntitlements	Erteilt die Berechtigung zum Abrufen von Berechtigungswerten für ein bestimmtes Produkt. Die Ergebnisse können basierend auf der Kunden-ID oder Produktdimensionen gefiltert werden.	Read			

Von AWS Marketplace Entitlement Service definierte Ressourcentypen

AWS Marketplace Der Entitlement Service unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource` Element einer IAM-Richtlinienanweisung. Um den Zugriff auf den AWS Marketplace Entitlement Service zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Marketplace Entitlement Service

Marketplace Entitlement hat keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace Image Building Service

AWS Marketplace Image Building Service (Servicepräfix: `aws-marketplace`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Marketplace Image Building Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den

Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeBuilds [nur Berechtigung]	Beschreibt Image-Builds, die durch eine Build-ID identifiziert wurden.	Read			
ListBuilds [nur Berechtigung]	Listet Image-Builds auf.	Read			
StartBuild [nur Berechtigung]	Startet einen Image-Build	Write			

Von AWS Marketplace Image Building Service definierte Ressourcentypen

AWS Marketplace Image Building Service unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf den AWS Marketplace Image Building Service zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Marketplace Image Building Service

Marketplace Image Build besitzt keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace Management Portal

AWS Marketplace Management Portal (Servicepräfix: `aws-marketplace-management`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Marketplace Management Portal definierte Aktionen
- Von AWS Marketplace Management Portal definierte Ressourcentypen
- Bedingungsschlüssel für AWS Marketplace Management Portal

Von AWS Marketplace Management Portal definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAdditionalSellerNotificationRecipients [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen weiterer Empfänger von Verkäufer benachrichtigungen	Lesen			
GetBankAccountVerificationDetails [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen des Verifizierungsstatus eines Bankkontos	Lesen			
GetSecondaryUserVerificationDetails [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen des Verifizierungsstatus eines sekundären Benutzerkontos	Lesen			
GetSellerVerificationDetail	Gewährt die Berechtigung zum Anzeigen des Verifizierungsstatus eines Kontos	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
s [nur Berechtigung]					
PutAdditionalSellerNotificationRecipients [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren weiterer Empfänger von Verkäufer benachrichtigungen	Schreiben			
PutBankAccountVerificationDetails [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren des Verifizierungsstatus eines Bankkontos	Schreiben			
PutSecondaryUserVerificationDetails [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren des Verifizierungsstatus eines sekundären Benutzerkontos	Schreiben			
PutSellerVerificationDetails [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren des Verifizierungsstatus eines Kontos	Schreiben			
uploadFiles [nur Berechtigung]	Gewährt Zugriff auf die Seite zum Hochladen von Dateien im AWS Marketplace Management Portal	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
viewMarketing [nur Berechtigung]	Gewährt Zugriff auf die Marketing-Seite im AWS Marketplace Management Portal	Auflisten			
viewReports [nur Berechtigung]	Gewährt Zugriff auf die Seite mit Berichten im AWS Marketplace Management Portal	Auflisten			
viewSettings [nur Berechtigung]	Gewährt Zugriff auf die Seite mit den Einstellungen im AWS Marketplace Management Portal	Auflisten			
viewSupport [nur Berechtigung]	Gewährt Zugriff auf die Seite zur Kundenservice-Berechtigung im AWS Marketplace Management Portal	Auflisten			

Von AWS Marketplace Management Portal definierte Ressourcentypen

AWS Marketplace Management Portal unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf AWS Marketplace Management Portal zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Marketplace Management Portal

Marketplace Portal besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace Metering Service

AWS Marketplace Metering Service (Servicepräfix: `aws-marketplace`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Marketplace Metering Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchMeterUsage	Gewährt die Erlaubnis zum Veröffentlichen von Metering-Datensätzen für eine Reihe von Kunden für SaaS-Anwendungen	Write			
MeterUsage	Gewährt die Berechtigung zum Ausgeben von Metering-Datensätzen	Write			
RegisterUsage	Gewährt die Berechtigung zum Überprüfen, ob der Kunde, der Ihre kostenpfl	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	ichtige Software ausführt, Ihr Produkt auf AWS Marketplace abonniert hat. So können Sie sich vor nicht autorisierter Nutzung schützen. Misst die Softwarenutzung pro ECS-Aufgabe, pro Stunde, mit auf einzelne Sekunden umgelegter Nutzung				
ResolveCustomer	Gewährt die Erlaubnis zum Auflösen eines Registrierungs-Tokens, um einen CustomerIdentifier und einen Produktcode zu erhalten	Write			

Von AWS Marketplace Metering Service definierte Ressourcentypen

AWS Marketplace Metering Service unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf AWS Marketplace Metering Service zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Marketplace Metering Service

Marketplace Metering umfasst keine servicespezifischen Kontextschlüssel, die im Element `Condition` von &IAM;-Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace Private Marketplace

AWS Marketplace Private Marketplace (Servicepräfix: `aws-marketplace`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Marketplace Private Marketplace definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateProductsWithPrivateMarketplace [nur Berechtigung]	Gewährt die Berechtigung zum Genehmigen einer Anfrage für ein Produkt, das dem Private Marketplace zugeordnet werden soll. Diese Aktion kann von jedem Konto in einer AWS-Organisation durchgeführt werden, sofern der Benutzer die entsprechenden Berechtigungen hat und die Servicekontrollrichtlinien der Organisation es zulassen.	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreatePrivateMarketplaceRequests [nur Berechtigung]	Erstellt eine neue Anfrage für ein oder mehrere Produkte, die dem Private Marketplace zugeordnet werden sollen. Diese Aktion kann von jedem Konto in einer AWS-Organisation durchgeführt werden, sofern der Benutzer über die entsprechenden Berechtigungen verfügt und die Service-Kontrollrichtlinien der Organisation dies zulassen.	Schreiben			
DescribePrivateMarketplaceRequests [nur Berechtigung]	Beschreibt Anfragen und zugehörige Produkte im Private Marketplace. Diese Aktion kann von jedem Konto in einer AWS-Organisation durchgeführt werden, sofern der Benutzer die entsprechenden Berechtigungen hat und die Servicekontrollrichtlinien der Organisation es zulassen.	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateProductsFromPrivateMarketplace [nur Berechtigung]	Gewährt die Berechtigung zum Ablehnen einer Anfrage für ein Produkt, die dem Private Marketplace zugeordnet werden soll. Diese Aktion kann von jedem Konto in einer AWS-Organisation durchgeführt werden, sofern der Benutzer die entsprechenden Berechtigungen hat und die Servicekontrollrichtlinien der Organisation es zulassen.	Schreiben			
ListPrivateMarketplaceRequests [nur Berechtigung]	Abfragbare Liste für Anfragen und zugehörige Produkte im Private Marketplace. Diese Aktion kann von jedem Konto in einer AWS-Organisation durchgeführt werden, sofern der Benutzer die entsprechenden Berechtigungen hat und die Servicekontrollrichtlinien der Organisation es zulassen.	Auflisten			

Von AWS Marketplace Private Marketplace definierte Ressourcentypen

AWS Marketplace Private Marketplace unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf AWS Marketplace Private Marketplace zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Marketplace Private Marketplace

Private Marketplace besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace Procurement Systems Integration

AWS Marketplace Procurement Systems Integration (Servicepräfix: `aws-marketplace`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Marketplace Procurement Systems Integration definierte Aktionen
- Von AWS Marketplace Procurement Systems Integration definierte Ressourcentypen
- Bedingungsschlüssel für AWS Marketplace Procurement Systems Integration

Von AWS Marketplace Procurement Systems Integration definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt,

müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeProcurementSystemConfiguration [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben der Procurement-System-Integration-Konfiguration (z. B. Coupa) für die einzelnen Konten oder für die gesamte	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	AWS-Organisation (falls vorhanden). Diese Aktion kann nur vom Masterkonto ausgeführt werden, wenn eine AWS-Organisation verwendet wird				
PutProcurementSystemConfiguration [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen oder Aktualisieren der Procurement-System-Integration-Konfiguration (z. B. Coupa) für die einzelnen Konten oder für die gesamte AWS-Organisation (falls vorhanden). Diese Aktion kann nur vom Masterkonto ausgeführt werden, wenn eine AWS-Organisation verwendet wird	Schreiben			

Von AWS Marketplace Procurement Systems Integration definierte Ressourcentypen

AWS Marketplace Procurement Systems Integration unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf AWS Marketplace Procurement Systems Integration zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Marketplace Procurement Systems Integration

Marketplace Procurement Integration besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Marketplace Seller Reporting

AWS Marketplace Seller Reporting (Servicepräfix: `aws-marketplace`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Marketplace Seller Reporting definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetSellerDashboard	Gewährt die Berechtigung zum Anzeigen eines Verkäufer-Dashboards	Lesen	SellerDashboard*		

Von AWS Marketplace Seller Reporting definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
SellerDashboard	`arn:${Partition}:aws-marketplace::${Account}:${Catalog}/ReportingData/${FactTable}/Dashboard/${DashboardName}`	

Bedingungsschlüssel für AWS Marketplace Seller Reporting

Marketplace Seller Reporting besitzt keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Zustandsschlüssel für AWS Marketplace Anbietereinblicke

AWS Marketplace Anbietereinblicke (Service-Präfix: `vendor-insights`) bietet die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Marketplace Anbietereinblicken definierte Aktionen
- Von AWS Marketplace Anbietereinblicken definierte Ressourcentypen
- Bedingungsschlüssel für AWS Marketplace Anbietereinblicke

Von AWS Marketplace Anbietereinblicken definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ActivateSecurityProfile	Erteilung der Berechtigung zur Aktivierung des Sicherheitsprofils	Schreiben	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
AssociateDataSource	Gewährt die Berechtigung, ein Sicherheitsprofil mit einer Datenquelle zu verknüpfen	Schreiben	SecurityProfile*		vendor-insights:GetDataSource
				aws:ResourceTag/${TagKey}	
CreateDataSource	Erteilung der Berechtigung zur Erstellung einer neuen Datenquelle	Schreiben		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	vendor-insights:TagResource
CreateSecurityProfile	Erteilung der Berechtigung zur Erstellung eines neuen Sicherheitsprofils	Schreiben		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey}	vendor-insights:TagResource

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
DeactivateSecurityProfile	Erteilung der Berechtigung zur Deaktivierung des Sicherheitsprofils	Schreiben	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
DeleteDataSource	Gewährt die Berechtigung zum Löschen einer Datenquelle	Schreiben	DataSource*		
				aws:ResourceTag/${TagKey}	
DisassociateDataSource	Erteilung der Berechtigung, das Sicherheitsprofil von einer Datenquelle zu trennen	Schreiben	SecurityProfile*		vendor-insights:GetDataSource
				aws:ResourceTag/${TagKey}	
GetDataSource	Erteilung der Berechtigung zum Abrufen der Details einer vorhandenen Datenquelle	Lesen	DataSource*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetEntitledSecurityProfileSnapshot	Erteilung der Berechtigung zur Rückgabe der Details eines Sicherheitsprofil-Snapshots, zu dessen Lesen der Anfragende berechtigt ist	Lesen	SecurityProfile*		
GetProfileAccessTerms	Erteilung der Berechtigung zum Abrufen der Zugriffsbedingungen für ein Anbietereinblicke-Profil	Lesen			
GetSecurityProfile	Erteilung der Berechtigung zur Rückgabe der Details eines bestehenden Sicherheitsprofils	Lesen	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
GetSecurityProfileSnapshot	Erteilung der Berechtigung zur Rückgabe der Details eines Sicherheitsprofil-Snapshots	Lesen	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
ListDataSources	Erteilung der Berechtigung, vorhandene Datenquellen aufzulisten	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListEntitledSecurityProfileSnapshots	Erteilung der Erlaubnis, die Snapshot-Zusammenfassungsliste für ein vorhandenes Sicherheitsprofil zurückzugeben, zu dessen Auflistung der Anfragende berechtigt ist	Auflisten	SecurityProfile*		
ListEntitledSecurityProfiles	Erteilung der Berechtigung, berechtigte Sicherheitsprofile aufzulisten	Auflisten			
ListSecurityProfileSnapshots	Erteilung der Berechtigung zur Rückgabe der Snapshot-Zusammenfassungsliste für ein vorhandenes Sicherheitsprofil	Auflisten	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
ListSecurityProfiles	Erteilung der Berechtigung, vorhandene Sicherheitsprofile aufzulisten	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für Anbietereinblicke	Lesen	DataSource		
			SecurityProfile		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Markieren der Anbieter-Insights-Ressource	Markierung	DataSource		
			SecurityProfile		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung der Anbieter-Insights-Ressource	Markierung	DataSource		
			SecurityProfile		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateDataSource	Gewährt die Berechtigung zum Aktualisieren einer vorhandenen Datenquelle	Schreiben	DataSource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
UpdateSecurityProfile	Erteilung der Berechtigung zur Aktualisierung des Sicherheitsprofils	Schreiben	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
UpdateSecurityProfileSnapshotCreationConfiguration	Gewährt die Berechtigung zum Aktualisieren der Konfiguration für die Erstellung von Sicherheitsprofil-Snapshots	Schreiben	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
UpdateSecurityProfileSnapshotReleaseConfiguration	Gewährt die Berechtigung zum Aktualisieren der Veröffentlichungskonfiguration des Sicherheitsprofil-Snapshots	Schreiben	SecurityProfile*		
				aws:ResourceTag/${TagKey}	

Von AWS Marketplace Anbietereinblicken definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
DataSource	`arn:${Partition}:vendor-insights:::data-source:${ResourceId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
SecurityProfile	`arn:${Partition}:vendor-insights:::security-profile:${ResourceId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Bedingungsschlüssel für AWS Marketplace Anbietereinblicke

AWS Marketplace Vendor Insights definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch Tags, die in der Anforderung übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf Tags, die der Ressource zugeordnet sind	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert den Zugriff basierend auf Tag-Schlüsseln, die in der Anforderung übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Mechanical Turk

Amazon Mechanical Turk (Servicepräfix: `mechanicalturk`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Mechanical Turk definierte Aktionen
- Von Amazon Mechanical Turk definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Mechanical Turk

Von Amazon Mechanical Turk definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptQualificationRequest	Die AcceptQualificationRequest-Produktion erlaubt die Anforderung eines	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Workers für eine Qualifizierung.				
ApproveAssignment	Die Produktion ApproveAssignment genehmigt die Ergebnisse einer abgeschlossenen Zuweisung.	Write			
AssociateQualificationWithWorker	Die AssociateQualificationWithWorker-Produktion gibt einem Worker eine Qualifizierung.	Write			
CreateAdditionalAssignmentsForHIT	Die CreateAdditionalAssignmentsForHIT-Produktion erhöht die maximale Anzahl von Zuweisungen einer vorhandenen HIT.	Write			
CreateHIT	Die Produktion CreateHIT erstellt eine neue Human Intelligence Task (HIT).	Write			
CreateHITType	Die CreateHITType-Produktion erstellt einen neuen HIT-Typ.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateHITWithHITType	Die CreateHITWithHITType-Produktion erstellt eine neue Human Intelligence Task (HIT) unter Verwendung einer vorhandenen HITTypeID, die durch die Produktion CreateHITType generiert wurde.	Write			
CreateQualificationType	Die Produktion CreateQualificationType erstellt einen neuen Qualifizierungstyp, der mittels einer QualificationType-Datenstruktur repräsentiert wird.	Write			
CreateWorkerBlock	Mit der Produktion CreateWorkerBlock können Sie verhindern, dass ein Worker an Ihren HITs arbeitet.	Write			
DeleteHIT	Die Produktion DeleteHIT entsorgt eine HIT, die nicht mehr benötigt wird.	Write			
DeleteQualificationType	Die Produktion DeleteQualificationType entsorgt einen Qualifizierungstyp sowie alle HIT-Typen, die dem Qualifizierungstyp zugeordnet sind.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteWorkerBlock	Mit der Produktion DeleteWorkerBlock können Sie die Sperre eines Workers aufheben, damit dieser wieder an Ihren HITs arbeiten kann.	Write			
DisassociateQualificationFromWorker	DisassociateQualificationFromWorker widerruft eine zuvor gewährte Qualifizierung von einem Benutzer.	Write			
GetAccountBalance	Die Produktion GetAccountBalance ruft den Geldbetrag des Amazon Mechanical Turk-Kontos ab.	Read			
GetAssignment	GetAssignment ruft unter Verwendung der Zuweisungs-ID eine Zuweisung mit einem AssignmentStatus-Wert von „Submitted“, „Approved“ oder „Rejected“ ab.	Read			
GetFileUploadURL	Die Produktion GetFileUploadURL generiert eine temporäre URL und gibt sie zurück.	Read			
GetHIT	Die Produktion GetHIT ruft die Details der angegebenen HIT ab.	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetQualificationScore	Die Produktion GetQualificationScore gibt den Wert der Qualifizierung eines Workers für einen gegebenen Qualifizierungstyp zurück.	Read			
GetQualificationType	Die Produktion GetQualificationType ruft Informationen zu einem Qualifizierungstyp über die ID ab.	Read			
ListAssignmentsForHIT	Die Produktion ListAssignmentsForHIT ruft abgeschlossene Zuweisungen für eine HIT ab.	List			
ListBonusPayments	Die Produktion ListBonusPayments ruft die Bonusbeträge ab, die Sie Workern für eine gegebene HIT oder eine Zuweisung gezahlt haben.	List			
ListHITs	Die ListHITs-Produktion gibt alle HITs eines Anforderers zurück.	List			
ListHITsForQualificationType	Die Produktion ListHITsForQualificationType gibt die HITs zurück, die den gegebenen Qualifizierungstyp für eine QualificationRequirement verwenden.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListQualificationRequests	Die Produktion ListQualificationRequests ruft Anforderungen für Qualifizierungen eines bestimmten Qualifizierungstyps ab.	List			
ListQualificationTypes	Die Produktion ListQualificationTypes sucht unter Verwendung der angegebenen Suchabfrage nach Qualifizierungstypen und gibt eine Liste der Qualifizierungstypen zurück.	List			
ListReviewPolicyResultsForHIT	Die Produktion ListReviewPolicyResultsForHIT ruft die berechneten Ergebnisse und zudem die Aktionen ab, die im Rahmen der Ausführung der Prüfrichtlinien während einer CreateHIT-Produktion durchgeführt wurden.	List			
ListReviewableHITs	Die ListReviewableHITs-Produktion gibt alle HITs eines Anforderers zurück, die nicht genehmigt oder abgelehnt wurden.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListWorkerBlocks	Die Produktion ListWorkersBlocks ruft eine Liste der Worker ab, die nicht an Ihren HITs arbeiten dürfen.	List			
ListWorkersWithQualificationType	Die ListWorkersWithQualificationType-Produktion gibt alle Worker eines bestimmten Qualifizierungstyps zurück.	List			
NotifyWorkers	Die Produktion NotifyWorkers sendet eine E-Mail an einzelne oder mehrere Worker, die Sie mit der Worker-ID angeben.	Write			
RejectAssignment	Die Produktion RejectAssignment weist die Ergebnisse einer abgeschlossenen Zuweisung zurück.	Write			
RejectQualificationRequest	Die Produktion RejectQualificationRequest weist die Anforderung einer Qualifizierung durch einen Benutzer zurück.	Write			
SendBonus	Die Produktion SendBonus veranlasst eine Geldzahlung von Ihrem Konto an einen Worker.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SendTestEventNotification	Die Produktion SendTestEventNotification veranlasst Amazon Mechanical Turk zum Senden einer Benachrichtigung wie bei einem HIT-Ereignis nach Maßgabe der angegebenen Benachrichtigungsspezifikation.	Write			
UpdateExpirationForHIT	Mit der UpdateExpirationForHIT-Produktion können Sie die Ablaufzeit einer HIT über die aktuellen Ablaufzeit hinaus verlängern oder eine HIT sofort ablaufen lassen.	Write			
UpdateHITReviewStatus	Die UpdateHITReviewStatus-Produktion schaltet den Status einer HIT um.	Write			
UpdateHITTypeOfHIT	Mit der UpdateHITTypeOfHIT-Produktion können Sie die HITType-Eigenschaften einer HIT ändern.	Write			
UpdateNotificationSettings	Die Produktion UpdateNotificationSettings erstellt, aktualisiert, deaktiviert oder reaktiviert Benachrichtigungen für einen HIT-Typ.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateQualificationType	Die Produktion UpdateQualificationType ändert die Attribute eines existierenden Qualifizierungstyps, der mittels einer QualificationType-Datenstruktur repräsentiert wird.	Write			

Von Amazon Mechanical Turk definierte Ressourcentypen

Amazon Mechanical Turk unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf Amazon Mechanical Turk zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für Amazon Mechanical Turk

MechanicalTurk besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Mobile Analytics

Amazon MemoryDB (Servicepräfix: `memorydb`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon DynamoDB definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

> **Note**
>
> Bei der Erstellung einer MemoryDB–for-Redis-Richtlinie in IAM, müssen Sie den Platzhalter "*" für den Ressourcenblock verwenden. Weitere Informationen zur Verwendung der folgenden MemoryDB für Redis-API-Aktionen in IAM-Richtlinien finden Sie unterMemoryDB-Aktionen und IAMaus.

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchUpdateCluster	Gewährt die Berechtigung zum Aktualisieren eines Service	Schreiben	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					s3:GetObject
				aws:ResourceTag/${TagKey}	
Connect	Ermöglicht es einem IAM-Benutzer oder einer -Rolle, sich als ein bestimmter MemoryDB-Benutzer mit einem Knoten in einem Cluster zu verbinden	Schreiben	cluster*		
			user*		
				aws:ResourceTag/${TagKey}	
CopySnapshot	Gewährt die Berechtigung zum Erstellen einer Kopie eines vorhandenen Snapshots	Schreiben	snapshot*		memorydb:TagResource s3:DeleteObject s3:GetBucketAcl s3:PutObject

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateAcl	Gewährt die Berechtigung zum Erstellen einer neuen Routenkontrolle	Schreiben	user*		memorydb:TagResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCluster	Gewährt die Berechtigung zum Erstellen eines Clusters	Schreiben	acl*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs memorydb:TagResource s3:GetObject
			parametergroup*		
			subnetgroup*		
			snapshot		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys memorydb:TLSEnabled	
CreateParameterGroup	Gewährt die Berechtigung zum Erstellen einer neuen DB-Parametergruppe	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	memorydb:TagResource
CreateSnapshot	Gewährt Berechtigungen zum Erstellen einer Sicherung eines Clusters zum aktuellen Zeitpunkt	Schreiben	cluster*		memorydb:TagResource s3:DeleteObject s3:GetBucketAcl s3:PutObject

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubnetGroup	Gewährt die Berechtigung zum Erstellen einer neuen DB-Subnetzgruppe	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	memorydb:TagResource
CreateUser	Gewährt die Berechtigung zum Erstellen eines neuen IAM-Benutzers.	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys memorydb:UserAuthenticationMode	memorydb:TagResource
DeleteAcl	Gewährt die Berechtigung zum Löschen einer Zugriffssteuerungsregel	Schreiben	acl*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
DeleteCluster	Gewährt die Berechtigung zum Löschen eines zuvor bereitgestellten Clusters	Schreiben	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			snapshot		
				aws:ResourceTag/${TagKey}	
DeleteParameterGroup	Gewährt die Berechtigung zum Erstellen einer Parametergruppe	Schreiben	parametergroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
DeleteSnapshot	Gewährt die Berechtigung zum Löschen eines manuellen Snapshots	Schreiben	snapshot*		
				aws:ResourceTag/${TagKey}	
DeleteSubnetGroup	Gewährt die Berechtigung zum Löschen einer Subnetzgruppe	Schreiben	subnetgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteUser	Gewährt die Berechtigung zum Löschen eines Benutzers	Schreiben	user*		
				aws:ResourceTag/${TagKey}	
DescribeAcls	Gewährt die Berechtigung zum Abrufen von Informationen über IP-Zugriffskontrollgruppen	Lesen	acl*		
				aws:ResourceTag/${TagKey}	
DescribeClusters	Die Aktion DescribeCacheClusters gibt Informationen über alle bereitgestellten Cache-Cluster zurück, wenn keine Cache-Cluster-Kennung angegeben ist, oder über einen bestimmten Cache-Cluster, wenn eine Cache-Cluster-Kennung bereitgestellt ist.	Lesen	cluster*		
				aws:ResourceTag/${TagKey}	
DescribeEngineVersions	Gewährt die Berechtigung zum Listen der verfügbaren Cache-Engines und deren Versionen	Lesen			
DescribeEvents	Gewährt die Berechtigung zum Auflisten von Ereignissen im Zusammenhang mit Clustern, Cache-Sicherheitsgruppen und Cache-Parametergruppen	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeParameterGroups	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Gruppe.	Lesen	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeParameters	Gewährt die Berechtigung zum Zurückgeben der detaillierten Parameterliste für eine bestimmte Cache-Parametergruppe	Lesen	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeReservedNodes	Gewährt Berechtigungen zum Abrufen von reservierten Knoten	Lesen	reservednode*		
				aws:ResourceTag/${TagKey}	
DescribeReservedNodesOfferings	Gewährt Berechtigungen zum Abrufen von Lösungen für reservierte Knoten	Lesen			
DescribeServiceUpdates	Gewährt die Berechtigung zum Auflisten von Details der Service-Updates	Lesen			
DescribeSnapshots	Gewährt die Berechtigung, Informationen über DB-Cluster-Snapshots zurückzugeben	Lesen	snapshot*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeSubnetGroups	Gewährt die Berechtigung zum Abrufen einer Liste der Gruppen.	Lesen	subnetgroup*		
				aws:ResourceTag/${TagKey}	
DescribeUsers	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Gruppe.	Lesen	user*		
				aws:ResourceTag/${TagKey}	
FailoverShard	Gewährt die Berechtigung zum Testen des automatischen Failovers für einen bestimmten Shard in einem Cluster	Schreiben	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
ListAllowedNodeTypeUpdates	Gewährt Berechtigungen zum Auflisten verfügbarer Knotentypupdates	Lesen	cluster*		
				aws:ResourceTag/${TagKey}	
ListTags	Gewährt die Berechtigung zum Auflisten aller Tags auf einer Ressource	Lesen	acl		
			cluster		
			parametergroup		
			snapshot		
			subnetgroup		
			user		
				aws:ResourceTag/${TagKey}	
PurchaseReservedNodesOffering	Gewährt Berechtigungen zum Kauf eines neuen reservierten Knotens	Schreiben	reservednode*		memorydb:TagResource

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
ResetParameterGroup	Gewährt die Berechtigung, die Parameter einer DB-Parametergruppe auf die Standardwerte der Engine/des Systems zurückzusetzen	Schreiben	parametergroup*		
				aws:ResourceTag/${TagKey}	
TagResource	Gewährt die Berechtigung zum Hinzufügen von bis zu 10 Kostenzuordnungs-Tags zu der benannten Ressource	Tagging	acl		
			cluster		
			parametergroup		
			reservednode		
			snapshot		
			subnetgroup		
			user		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Erteilt Berechtigungen zum Entfernen der in der TagKeys Liste identifizierten Tags aus einer Ressource	Tagging	acl		
			cluster		
			parametergroup		
			snapshot		
			subnetgroup		
			user		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateAcl	Gewährt die Berechtigung zum Auflisten der Zugriffssteuerungsregeln	Schreiben	acl*		
			user*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
UpdateCluster	Gewährt die Berechtigung zum Aktualisieren der Überwachungseinstellungen für den MSK-Cluster	Schreiben	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			acl		
			parameter group		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateParameterGroup	Gewährt die Berechtigung zum Ändern der Parameter einer Parametergruppe	Schreiben	parametergroup*		
				aws:ResourceTag/${TagKey}	
UpdateSubnetGroup	Gewährt die Berechtigung zum Aktualisieren einer Gruppe.	Schreiben	subnetgroup*		
				aws:ResourceTag/${TagKey}	
UpdateUser	Gewährt die Berechtigung zum Aktualisieren eines Benutzerprofils	Schreiben	user*		
				aws:ResourceTag/${TagKey} memorydb:UserAuthenticationMode	

Von Amazon Translate definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
parametergroup	`arn:${Partition}:memorydb:${Region}:${Account}:parametergroup/${ParameterGroupName}`	aws:ResourceTag/${TagKey}
subnetgroup	`arn:${Partition}:memorydb:${Region}:${Account}:subnetgroup/${SubnetGroupName}`	aws:ResourceTag/${TagKey}
cluster	`arn:${Partition}:memorydb:${Region}:${Account}:cluster/${ClusterName}`	aws:ResourceTag/${TagKey}
snapshot	`arn:${Partition}:memorydb:${Region}:${Account}:snapshot/${SnapshotName}`	aws:ResourceTag/${TagKey}
user	`arn:${Partition}:memorydb:${Region}:${Account}:user/${UserName}`	aws:ResourceTag/${TagKey}
acl	`arn:${Partition}:memorydb:${Region}:${Account}:acl/${AclName}`	aws:ResourceTag/${TagKey}
reservednode	`arn:${Partition}:memorydb:${Region}:${Account}:reservednode/${ReservationID}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon DynamoDB

Amazon Pinpoint Email Service definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf den Markierungen, die in der Anforderung übergeben werden.	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf den Markierungen, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert Aktionen basierend auf den Tag-Schlüsseln, die in der Anforderung übergeben werden.	ArrayOfString
memorydb:TLSEnabled	Filtert den Zugriff nach dem in der Anfrage vorhandenen TlsEnabled-Parameter oder verwendet standardmäßig den Wert true, wenn der Parameter nicht vorhanden ist	Bool
memorydb:UserAuthenticationMode	Filtert den Zugriff nach dem UserAuthentication Mode .Type-Parameter in der Anfrage	String

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Message Delivery Service

Amazon Message Delivery Service (Servicepräfix: `ec2messages`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Message Delivery Service definierte Aktionen
- Von Amazon Message Delivery Service definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Message Delivery Service

Von Amazon Message Delivery Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcknowledgeMessage	Gewährt die Berechtigung zum Bestätigen einer Nachricht, wobei sichergestellt wird, dass sie nicht erneut zugestellt wird	Write			
DeleteMessage	Gewährt die Berechtigung zum Löschen einer Nachricht	Write			
FailMessage	Gewährt die Berechtigung eine Mitteilung fehlschlagen zu lassen, was bedeutet, dass die Mitteilung nicht erfolgreich verarbeitet werden konnte, wobei sichergestellt wird, dass sie nicht beantwortet werden kann, und nicht erneut zugestellt wird	Write			
GetEndpoint	Gewährt die Berechtigung zum Weiterleiten des Datenverkehrs an den richtigen Endpunkt basierend auf dem gegebenen Ziel der Mitteilungen	Read			
GetMessages	Gewährt die Berechtigung zum Übermitteln von Nachrichten für Clients/Instances mittels Langabfrage	Read		ssm:SourceInstanceARN	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ec2:SourceInstanceARN	
SendReply	Gewährt die Berechtigung zum Senden von Antworten von Clients/Instances an den Upstream-Service	Write		ssm:SourceInstanceARN ec2:SourceInstanceARN	

Von Amazon Message Delivery Service definierte Ressourcentypen

Amazon Message Delivery Service unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf Amazon Message Delivery Service zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für Amazon Message Delivery Service

Amazon Message Delivery Service definiert die folgenden Bedingungsschlüssel, die in einem `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
ec2:SourceInstanceARN	Filtert den Zugriff nach ARN der Instance, von der die Anforderung stammt	ARN
ssm:SourceInstanceARN	Filtert den Zugriff durch Überprüfung des Amazon-Ressourcenname (ARN) der verwalteten Instance des AWS Systems Managers, von der aus die Instance gestellt wird. Dieser Schlüssel ist nicht vorhanden, wenn die Instance von der verwalteten Instance kommt, die mit einer IAM-Rolle authentifiziert wurde, die dem EC2-Instance-Profil zugeordnet ist	ARN

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Message Gateway Service

Amazon Message Gateway Service (Servicepräfix: `ssmmessages`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Message Gateway Service definierte Aktionen
- Von Amazon Message Gateway Service definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Message Gateway Service

Von Amazon Message Gateway Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateControlChannel	Gewährt die Berechtigung zum Registrieren eines Steuerungskanals für eine Instance zum Senden von Steuerungsnachrichten an den Systems Manager-Service	Write		ssm:SourceInstanceARN ec2:SourceInstanceARN	
CreateDataChannel	Gewährt die Berechtigung zum Registrieren eines Datenkanals für eine Instance zum Senden von Datennachrichten an den Systems Manager-Service	Write			
OpenControlChannel	Gewährt die Berechtigung zum Öffnen einer Websocket-Verbindung für einen registrierten Steuerungskanal-Stream aus einer Instance zum Systems Manager-Service	Write			
OpenDataChannel	Gewährt die Berechtigung zum Öffnen eine Websocket-Verbindung für einen registrierten Datenkanal-Stream aus einer Instance zum Systems Manager-Service	Schreiben			

Von Amazon Message Gateway Service definierte Ressourcentypen

Amazon Message Gateway Service unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`Element einer IAM-Richtlinienanweisung. Um den Zugriff auf Amazon Message Gateway Service zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für Amazon Message Gateway Service

Amazon Message Gateway Service definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
ec2:SourceInstanceARN	Filtert den Zugriff nach ARN der Instance, von der die Anforderung stammt	ARN
ssm:SourceInstanceARN	Filtert den Zugriff durch Überprüfen des Amazon-Ressourcennamens (ARN) der verwalteten Instance des AWS Systems Managers, von der aus die Anforderung gestellt wird. Dieser Schlüssel ist nicht vorhanden, wenn die Instance von der verwalteten Instance kommt, die mit einer IAM-Rolle authentifiziert wurde, die dem EC2-Instance-Profil zugeordnet ist	ARN

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Microservice Extractor für .NET

AWS Microservice Extractor für .NET (Servicepräfix: `serviceextract`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Microservice Extractor für .NET definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetConfig [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen der erforderlichen Konfiguration für den Desktop-Client von AWS Microservice Extractor für .NET	Lesen			

Von AWS Microservice Extractor für .NET definierte Ressourcentypen

AWS Microservice Extractor für .NET unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf AWS Microservice Extractor für .NET zu gewähren, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Microservice Extractor für .NET

Microservice Extractor für .NET umfasst keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS-Guthaben für das Programm zur Migrationsbeschleunigung

AWS-Guthaben für das Programm zur Migrationsbeschleunigung (Service-Präfix: `mapcredits`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Richtlinien für Berechtigungen bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Durch AWS-Guthaben des Programms zur Migrationsbeschleunigung definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie

den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAssociatedPrograms [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen der zugehörigen Programm-Vereinbarungen zur Migrationsbeschleunigung des Benutzers	Auflisten	agreement*		
ListQuarterCredits [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen der mit dem Zahlerkonto des Benutzers verknüpften Guthaben für Programm-Vereinbarungen zur Migrationsbeschleunigung	Auflisten	agreement*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListQuarterSpend [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen berechtigter Ausgaben für Programm-Vereinbarungen zur Migrationsbeschleunigung, die mit dem Zahlerkonto des Benutzers verknüpft sind	Auflisten	agreement *		

Durch AWS-Guthaben des Programms zur Migrationsbeschleunigung definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
agreement	`arn:${Partition}:mapcredits:::${Agreement}/${AgreementId}`	

Konditionsschlüssel für AWS-Guthaben des Programms zur Migrationsbeschleunigung

MapCredits verfügt über keine servicespezifischen Kontextschlüssel, die im `Condition`-Element der Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Migration Hub

AWS Migration Hub (Servicepräfix: `mgh`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Migration Hub definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateCreatedArtifact	Gewährt die Berechtigung zum Verknüpfen eines bestimmten AWS-Artefakts mit einer MigrationTask	Schreiben	migrationTask*		
AssociateDiscoveredResource	Gewährt die Berechtigung zum Verknüpfen einer ADR-Ressource mit einer Migration Task	Schreiben	migrationTask*		
CreateHomeRegionControl	Gewährt die Berechtigung zum Erstellen einer Home-Regionssteuerung des Migration Hub	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateProgressUpdateStream	Gewährt die Berechtigung zum Erstellen eines ProgressUpdateStream	Schreiben	progressUpdateStream*		
DeleteHomeRegionControl	Gewährt die Berechtigung zum Löschen einer Home-Regionssteuerung des Migration Hub	Schreiben			
DeleteProgressUpdateStream	Gewährt die Berechtigung zum Löschen eines ProgressUpdateStream	Schreiben	progressUpdateStream*		
DescribeApplicationState	Gewährt die Berechtigung zum Abrufen des Zustands einer Application-Discovery-Service-Anwendung	Lesen			
DescribeHomeRegionControls	Gewährt die Berechtigung zum Auflisten von Home-Regionssteuerungen	Auflisten			
DescribeMigrationTask	Gewährt die Berechtigung zum Beschreiben einer MigrationTask	Lesen	migrationTask*		
DisassociateCreatedArtifact	Gewährt die Berechtigung zum Trennen der Verknüpfung eines bestimmten AWS-Artefakts mit einer MigrationTask	Schreiben	migrationTask*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateDiscoveredResource	Gewährt die Berechtigung zum Trennen der Verknüpfung einer ADR-Ressource mit einer MigrationTask	Schreiben	migrationTask*		
GetHomeRegion	Gewährt die Berechtigung zum Abrufen einer Home-Regionssteuerung des Migration Hub	Lesen			
ImportMigrationTask	Gewährt die Berechtigung zum Importieren einer MigrationTask	Schreiben	migrationTask*		
ListApplicationStates	Gewährt die Berechtigung zum Auflisten des Zustands von Anwendungen	Auflisten			
ListCreatedArtifacts	Gewährt die Berechtigung zum Auflisten verknüpfter, erstellter Artefakte für eine MigrationTask	Auflisten	migrationTask*		
ListDiscoveredResources	Gewährt die Berechtigung zum Auflisten verknüpfter ADR-Ressourcen mit einer MigrationTask	Auflisten	migrationTask*		
ListMigrationTasks	Gewährt die Berechtigung zum Auflisten von Migration Tasks	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListProgressUpdateStreams	Gewährt die Berechtigung zum Auflisten von ProgressUpdateStreams	Auflisten			
NotifyApplicationState	Gewährt die Berechtigung zum Aktualisieren des Zustands einer Application-Discovery-Service-Anwendung	Schreiben			
NotifyMigrationTaskState	Gewährt die Berechtigung zum Benachrichtigen des aktuellen Zustands der MigrationTask	Schreiben	migrationTask*		
PutResourceAttributes	Gewährt die Berechtigung zum Festlegen von ResourceAttributes	Schreiben	migrationTask*		

Vom AWS Migration Hub definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
progressUpdateStream	`arn:${Partition}:mgh:${Region}:${Account}:progressUpdateStream/${Stream}`	

Ressource ntypen	ARN	Bedingungsschlüssel
migration Task	`arn:${Partition}:mgh:${Region}:${Account}:progressUpdateStream/${Stream}/migrationTask/${Task}`	

Bedingungsschlüssel für AWS Migration Hub

Migration Hub besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Migration Hub Orchestrator

AWS Migration Hub Orchestrator (Dienstpräfix:`migrationhub-orchestrator`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Migration Hub Orchestrator definierte Aktionen
- Vom AWS Migration Hub Orchestrator definierte Ressourcentypen
- Bedingungsschlüssel für AWS Migration Hub Orchestrator

Von AWS Migration Hub Orchestrator definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen.

Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTemplate	Erteilt die Berechtigung zum Erstellen einer benutzerdefinierten Vorlage	Schreiben			
CreateWorkflow	Gewährt die Berechtigung zum Erstellen eines Workflows basierend auf der ausgewählten Vorlage	Schreiben	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkflowStep	Gewährt die Berechtigung zum Erstellen eines Schritts unter einem Workflow und einer bestimmten Schrittgruppe	Schreiben	workflow*		
CreateWorkflowStepGroup	Gewährt die Berechtigung zum Erstellen einer benutzerdefinierten Schrittgruppe für einen bestimmten Workflow	Schreiben	workflow*		
DeleteTemplate	Erteilt die Berechtigung zum Löschen einer benutzerdefinierten Vorlage	Schreiben	template*		
DeleteWorkflow	Gewährt die Berechtigung für einen Workflow	Schreiben	workflow*		
DeleteWorkflowStep	Gewährt die Berechtigung zum Löschen eines Schritts	Schreiben	workflow*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	aus einer bestimmten Schrittgruppe unter einem Workflow				
DeleteWorkflowStepGroup	Gewährt die Berechtigung zum Löschen einer mit einem Workflow verknüpften Schrittgruppe	Schreiben	workflow*		
GetMessage	Gewährt dem Plug-In die Berechtigung, Informationen vom Service zu erhalten	Lesen			
GetTemplate	Gewährt die Berechtigung zum Abrufen von Metadaten für eine Vorlage	Lesen	template*		
GetTemplateStep	Gewährt die Berechtigung zum Abrufen von Details eines Schritts, der mit einer Vorlage und einer Schrittgruppe verknüpft ist	Lesen	template*		
GetTemplateStepGroup	Gewährt die Berechtigung zum Abrufen von Metadaten einer Schrittgruppe unter einer Vorlage	Lesen	template*		
GetWorkflow	Gewährt die Berechtigung zum Abrufen von Metadaten, die mit einem Workflow verknüpft sind	Lesen	workflow*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetWorkflowStep	Gewährt die Berechtigung zum Abrufen von Details eines Schritts, der mit einem Workflow und einer Schrittgruppe verknüpft sind	Lesen	workflow*		
GetWorkflowStepGroup	Gewährt die Berechtigung zum Abrufen von Details einer mit einem Workflow verknüpften Schrittgruppe	Lesen	workflow*		
ListPlugins	Gewährt die Berechtigung zum Abrufen einer Liste aller registrierten Plug-Ins	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Abrufen einer Liste aller mit einer Ressource verknüpften Tags	Lesen	template* workflow*		
ListTemplateStepGroups	Gewährt die Berechtigung zum Auflisten der Schrittgruppen einer Vorlage	Auflisten	template*		
ListTemplateSteps	Gewährt die Berechtigung zum Abrufen einer Liste von Schritten in einer Schrittgruppe	Auflisten	template*		
ListTemplates	Gewährt die Berechtigung zum Abrufen einer Liste aller Vorlagen, die dem Kunden zur Verfügung stehen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListWorkflowStepGroups	Gewährt die Berechtigung zum Abrufen einer Liste von Schrittgruppen, die mit einem Workflow verknüpft sind	Auflisten	workflow*		
ListWorkflowSteps	Gewährt die Berechtigung zum Abrufen einer Liste von Schritten in einer mit einem Workflow verknüpften Schrittgruppe	Auflisten	workflow*		
ListWorkflows	Gewährt die Berechtigung zum Auflisten aller Workflows	Auflisten			
RegisterPlugin	Gewährt die Berechtigung zum Registrieren des Plug-Ins, um eine ID zu erhalten und Nachrichten vom Service zu empfangen	Schreiben			
RetryWorkflowStep	Gewährt die Berechtigung zum Wiederholen eines fehlgeschlagenen Schritts innerhalb eines Workflows	Schreiben	workflow*		
SendMessage	Gewährt dem Plug-In die Berechtigung, Informationen an den Service zu senden	Schreiben			
StartWorkflow	Gewährt die Berechtigung zum Starten eines Workflows oder zum Fortsetzen eines angehaltenen Workflows	Schreiben	workflow*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopWorkflow	Gewährt die Berechtigung zum Anhalten eines Workflows	Schreiben	workflow*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Ressource	Markieren	template		
			workflow		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Ressource	Tagging	template		
			workflow		
				aws:TagKeys	
UpdateTemplate	Erteilt die Berechtigung zum Aktualisieren einer benutzerdefinierten Vorlage	Schreiben	template*		
UpdateWorkflow	Gewährt die Berechtigung zum Aktualisieren der mit dem Workflow verknüpften Metadaten	Schreiben	workflow*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateWorkflowStep	Gewährt die Berechtigung zum Aktualisieren der Metadaten und des Status eines benutzerdefinierten Schritts innerhalb eines Workflows	Schreiben	workflow*		
UpdateWorkflowStepGroup	Gewährt die Berechtigung zum Aktualisieren von Metadaten, die in einem Workflow mit einer Schrittgruppe verknüpft sind	Schreiben	workflow*		

Vom AWS Migration Hub Orchestrator definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
workflow	`arn:${Partition}:migrationhub-orchestrator:${Region}:${Account}:workflow/${ResourceId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
template	`arn:${Partition}:migrationhub-orchestrator:${Region}:${Account}:template/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Migration Hub Orchestrator

AWS Migration Hub Orchestrator definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Migration Hub Refactor Spaces

AWS Migration Hub Refactor Spaces (Servicepräfix: `refactor-spaces`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Migration Hub Refactor Spaces definierte Aktionen
- Vom AWS Migration Hub Refactor Spaces definierte Ressourcentypen
- Bedingungsschlüssel für AWS Migration Hub Refactor Spaces

Von AWS Migration Hub Refactor Spaces definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateApplication	Gewährt die Berechtigung zum Erstellen einer Anwendung innerhalb einer Umgebung	Schreiben		refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateEnvironment	Gewährt die Berechtigung zum Erstellen einer Umgebung	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateRoute	Gewährt die Berechtigung zum Erstellen einer Route in einer Anwendung	Schreiben		refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateService	Gewährt die Berechtigung zum Erstellen eines Services in einer Anwendung	Schreiben		refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:CreatedByAccountIds aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Gewährt die Berechtigung zum Löschen einer Anwendung aus einer Umgebung	Schreiben	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
DeleteEnvironment	Gewährt die Berechtigung zum Löschen einer Umgebung	Schreiben	environment*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	Gewährt die Berechtigung zum Löschen einer Ressourcenrichtlinie	Schreiben			
DeleteRoute	Gewährt die Berechtigung zum Löschen einer Route aus einer Anwendung	Schreiben	route*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:ResourceTag/${TagKey}	
DeleteService		Schreiben	service*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Gewährt die Berechtigung zum Löschen eines Services aus einer Anwendung			refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
GetApplication	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Anwendung	Lesen	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
GetEnvironment	Gewährt die Berechtigung zum Abrufen von Informationen für eine Umgebung	Lesen	environment*		
				aws:ResourceTag/${TagKey}	
GetResourcePolicy	Gewährt die Berechtigung zum Abrufen von Details über eine Ressourcen-Richtlinie	Lesen			
GetRoute	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Route	Lesen	route*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetService	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Service	Lesen	service*		
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
ListApplications	Gewährt die Berechtigung zum Auflisten aller Anwendungen in einer Umgebung	Lesen	application*		
ListEnvironmentVpcs	Gewährt die Berechtigung zum Auflisten aller VPCs für die Umgebung	Lesen	environment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListEnvironments	Gewährt die Berechtigung zum Auflisten aller Umgebungen	Lesen			
ListRoutes	Gewährt die Berechtigung zum Auflisten aller Routen in einer Anwendung	Lesen	route*		
ListServices	Gewährt die Berechtigung zum Auflisten aller Services in einer Umgebung	Lesen	environment*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten aller Tags für eine angegebene Ressource	Lesen			
PutResourcePolicy	Gewährt die Berechtigung zum Hinzufügen einer Ressourcenrichtlinie	Schreiben			
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markierung	application		
			environment		
			route		
			service		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen eines Tags von einer Ressource	Markierung	application		
			environment		
			route		
			service		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
UpdateRoute	Gewährt die Berechtigung zum Aktualisieren einer Route aus einer Anwendung	Schreiben	route*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:ResourceTag/${TagKey}	

Vom AWS Migration Hub Refactor Spaces definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
environment	`arn:${Partition}:refactor-spaces:${Region}:${Account}:environment/${EnvironmentId}`	aws:ResourceTag/${TagKey}
application	`arn:${Partition}:refactor-spaces:${Region}:${Account}:environment/${EnvironmentId}/application/${ApplicationId}`	aws:ResourceTag/${TagKey} refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds
service	`arn:${Partition}:refactor-spaces:${Region}:${Account}:environment/${EnvironmentId}/application/${ApplicationId}/service/${ServiceId}`	aws:ResourceTag/${TagKey} refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:ServiceCreatedByAccount

Ressourcentypen	ARN	Bedingungsschlüssel
route	`arn:${Partition}:refactor-spaces:${Region}:${Account}:environment/${EnvironmentId}/application/${ApplicationId}/route/${RouteId}`	aws:ResourceTag/${TagKey} refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:RouteCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:SourcePath

Bedingungsschlüssel für AWS Migration Hub Refactor Spaces

AWS Migration Hub Refactor Spaces definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString
refactor-spaces:ApplicationCreatedByAccount	Filtert den Zugriff, indem die Aktion nur auf die Konten beschränkt wird, die die Anwendung in einer Umgebung erstellt haben	Zeichenfolge
refactor-spaces:CreatedByAccountIds	Filtert den Zugriff nach den Konten, die die Ressource erstellt haben	ArrayOfString
refactor-spaces:RouteCreatedByAccount	Filtert den Zugriff, indem die Aktion nur auf die Konten beschränkt wird, die die Route in einer Anwendung erstellt haben	Zeichenfolge
refactor-spaces:ServiceCreatedByAccount	Filtert den Zugriff, indem die Aktion nur auf die Konten beschränkt wird, die den Service in einer Anwendung erstellt haben	Zeichenfolge
refactor-spaces:SourcePath	Filtert den Zugriff nach dem Pfad der Route	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Migration Hub Strategy Recommendations

AWS Migration Hub Strategy Recommendations (Servicepräfix: `migrationhub-strategy`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Migration Hub Strategy Recommendations definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAntiPattern	Gewährt die Berechtigung, Details zu jedem Anti-Muster abzurufen, das der Samller in der Umgebung eines Kunden prüfen sollte	Lesen			
GetApplicationComponentDetails	Gewährt die Berechtigung, Details zu einer Anwendung zu erhalten	Lesen			
GetApplicationComp	Gewährt die Berechtigung zum Abrufen einer Liste aller empfohlenen Strategien und	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
onentStrategies	Tools für eine Anwendung, die auf einem Server ausgeführt wird				
GetAssessment	Gewährt die Berechtigung zum Abrufen des Status einer laufenden Bewertung	Lesen			
GetImportFileTask	Gewährt die Berechtigung zum Abrufen von Details zu einer bestimmten Importaufgabe	Lesen			
GetLatestAssessmentId	Erteilt die Berechtigung zum Abrufen der aktuellsten Bewertungs-ID	Lesen			
GetMessage	Gewährt dem Sammler die Berechtigung, Informationen vom Service zu erhalten	Lesen			
GetPortfolioPreferences	Gewährt die Berechtigung zum Abrufen von Einstellungen für Kundenmigration/-modernisierung	Lesen			
GetPortfolioSummary	Gewährt die Berechtigung zum Abrufen der Gesamtzusammenfassung (Anzahl der Server, die neu gehostet werden sollen usw. sowie Gesamtzahl der Anti-Muster)	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetRecommendationReportDetails	Gewährt die Berechtigung zum Abrufen detaillierter Informationen zu einem Empfehlungsbericht	Lesen			
GetServerDetails	Gewährt die Berechtigung zum Abrufen von Informationen zu einem bestimmten Server	Lesen			
GetServerStrategies	Gewährt die Berechtigung zum Abrufen von empfohlenen Strategien und Tools für einen bestimmten Server	Lesen			
ListAnalyzableServers	Gewährt die Berechtigung zum Abrufen einer Liste aller analysierbarer Server in der VCenter-Umgebung eines Kunden	Auflisten			
ListAntiPatterns	Gewährt die Berechtigung zum Abrufen einer Liste aller Anti-Muster, nach denen der Sammler in der Umgebung eines Kunden suchen sollte	Auflisten			
ListApplicationComponents	Gewährt die Berechtigung zum Abrufen einer Liste aller Anwendungen, die auf Servern auf den Servern des Kunden ausgeführt werden	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListCollectors	Gewährt die Berechtigung zum Abrufen einer Liste aller vom Kunden installierten Sammlers	Auflisten			
ListImportFileTask	Gewährt die Erlaubnis, eine Liste aller vom Kunden durchgeführten Importe zu erhalten	Auflisten			
ListJarArtifacts	Gewährt die Berechtigung zum Abrufen einer Liste von Binärdateien, die der Sammler bewerten sollte	Auflisten			
ListServers	Gewährt die Berechtigung zum Abrufen einer Liste aller Server in der Umgebung eines Kunden	Auflisten			
PutLogData	Gewährt dem Kollektor die Berechtigung zum Senden von Protokollen an den Service	Schreiben			
PutMetricData	Gewährt dem Kollektor die Berechtigung zum Senden von Metriken an den Service	Schreiben			
PutPortfolioPreferences	Gewährt die Berechtigung zum Speichern der Migration/Modernisierungseinstellungen des Kunden	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RegisterCollector	Gewährt die Erlaubnis, den Sammler zu registrieren, um eine ID zu erhalten und Nachrichten vom Service zu empfangen	Schreiben			
SendMessage	Gewährt dem Sammler die Berechtigung, Informationen an den Service zu senden	Schreiben			
StartAssessment	Gewährt die Erlaubnis, die Bewertung in der Umgebung eines Kunden zu beginnen (Daten von allen Servern zu sammeln und Empfehlungen zu geben)	Schreiben			
StartImportFileTask	Gewährt die Erlaubnis, Daten aus einer vom Kunden bereitgestellten Datei zu importieren	Schreiben			
StartRecommendationReportGeneration	Gewährt die Berechtigung zum Erstellen eines Empfehlungsberichts	Schreiben			
StopAssessment	Gewährt die Erlaubnis, eine laufende Bewertung zu stoppen	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateApplicationComponentConfig	Gewährt die Berechtigung zum Aktualisieren der Details für eine Anwendung	Schreiben			
UpdateCollectorConfiguration	Erteilt dem Sammler die Berechtigung, Konfigurationen an den Service zu senden	Schreiben			
UpdateServerConfig	Gewährt die Berechtigung, Informationen auf einem Server zusammen mit der empfohlenen Strategie zu aktualisieren	Schreiben			

Von AWS Migration Hub Strategy Recommendations definierte Ressourcentypen

AWS Migration Hub Strategy Recommendations unterstützt nicht die Angabe eines Ressourcen-ARN im -`Resource`Element einer IAM-Richtlinienanweisung. Um Zugriff auf AWS Migration Hub Strategy Recommendations zu gewähren, geben Sie `"Resource": "*"` in einer Richtlinie an.

Bedingungsschlüssel für AWS Migration Hub Strategy Recommendations

Migration Hub Strategy Recommendations besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Mobile Analytics

Amazon Mobile Analytics (Servicepräfix: `mobileanalytics`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Mobile Analytics definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetFinancialReports	Gewähren des Zugriffs auf finanzielle Metriken für eine App	Read			
GetReports	Gewähren des Zugriffs auf Standardmetriken für eine App	Read			
PutEvents	Die PutEvents-Produktion zeichnet ein oder mehrere Ereignisse auf.	Write			

Von Amazon Mobile Analytics definierte Ressourcentypen

Amazon Mobile Analytics unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf Amazon Mobile Analytics zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für Amazon Mobile Analytics

Mobile Analytics umfasst keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Monitron

Amazon Monitron (Servicepräfix: `monitron`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Monitron definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateProjectAdminUser [nur Berechtigung]	Gewährt die Berechtigung, dem Projekt einen Benutzer als Administrator zuzuordnen	Berechtigungsverwaltung	project*		sso-directory:DescribeUsers

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					sso:AssociateProfile sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfileAssociations sso:ListProfiles

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateProject [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines Projekts	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole kms:CreateGrant sso:CreateManagedApplicationInstance sso:DeleteManagedApplicationInstance sso:DescribeRegisteredRegions

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateProjectUserAssociation [nur Berechtigung]	Gewährt die Berechtigung zum Zuordnen eines Benutzers zum Projekt	Berechtigungsverwaltung	project*		sso-directory:DescribeUsers sso:AssociateProfile sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfileAssociations sso:ListProfiles

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateUserAccessRoleAssociation [nur Berechtigung]	Gewährt die Berechtigung zum Zuordnen einer Zugriffsrolle zum Benutzer	Berechtigungsverwaltung	project*		sso-directory:DescribeUsers sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfileAssociations sso:ListProfiles
DeleteProject [nur Berechtigung]	Gewährt die Berechtigung zum Löschen eines Projekts	Write	project*		sso:DeleteManagedApplicationInstance

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteProjectUserAssociation [nur Berechtigung]	Gewährt die Berechtigung zum Trennen eines Benutzers vom Projekt	Berechtigungsverwaltung	project*		sso-directory:DescribeUsers sso:DisassociateProfile sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfiles
DeleteUserAccessRoleAssociation [nur Berechtigung]	Gewährt die Berechtigung zum Trennen einer Zugriffsrolle vom Benutzer	Berechtigungsverwaltung	project*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateProjectAdminUser [nur Berechtigung]	Gewährt die Berechtigung, die Mapping eines Administrators zum Projekt aufzuheben	Berechtigungsverwaltung	project*		sso-directory:DescribeUsers sso:DisassociateProfile sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfiles
GetProject [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Projekt	Read	project*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetProjectAdminUser [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben eines Administrators, der dem Projekt zugeordnet ist	Read	project*		sso-directory:DescribeUsers sso:GetManagedApplicationInstance sso:ListProfileAssociations
ListProjectAdminUsers [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aller Administratoren, die dem Projekt zugeordnet sind	Berechtigungsverwaltung	project*		sso-directory:DescribeUsers sso:GetManagedApplicationInstance

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListProjectUserAssociations [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aller Benutzer, die dem Projekt zugeordnet sind	Auflisten	project*		sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfileAssociations sso:ListProfiles
ListProjects [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aller Projekte	List			
ListTagsForResource [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aller Tags für eine Ressource	Read	project		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListUserAccessRoleAssociations [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aller Zugriffsrollen, die dem Benutzer zugeordnet sind	Auflisten	project*		
TagResource [nur Berechtigung]	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren	project		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [nur Berechtigung]	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Markieren	project		
				aws:TagKeys	
UpdateProject [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren eines Projekts	Write	project*		

Von Amazon Monitron definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
project	`arn:${Partition}:monitron:${Region}:${Account}:project/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Monitron

Amazon Monitron definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tag-Schlüssel-Wert-Paare in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff über die Tags, die an die Ressource angehängt sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon MQ

Amazon MQ (Servicepräfix: `mq`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.

- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon MQ definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateBroker	Gewährt die Berechtigung zum Erstellen eines Brokers	Write		aws:RequestTag/${TagKey}	ec2:CreateNetworkInterface
				aws:TagKeys	ec2:CreateNetworkInterfacePermission
					ec2:CreateSecurityGroup
					ec2:CreateVpcEndpoint
					ec2:DescribeInternetGateways

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ec2:DescribeNetworkInterfacePermissions ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyNetworkInterfaceAttribute iam:CreateServiceLinkedRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					route53:AssociateVPCWithHostedZone
CreateConfiguration	Gewährt die Berechtigung zum Erstellen einer Konfiguration für den angegebenen Konfigurationsnamen. Amazon MQ verwendet die Standardkonfiguration (Engine-Typ und Engine-Version).	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateReplicaBroker [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines Replica-Brokers	Schreiben	brokers*		
CreateTags	Gewährt die Berechtigung zum Erstellen von Tags	Markieren	brokers		
			configurations		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUser	Gewährt die Berechtigung zum Erstellen eines ActiveMQ-Benutzers	Write	brokers*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteBroker	Gewährt die Berechtigung zum Löschen eines Brokers	Write	brokers*		ec2:DeleteNetworkInterface ec2:DeleteNetworkInterfacePermission ec2:DeleteVpcEndpoints ec2:DetachNetworkInterface
DeleteTags	Gewährt die Berechtigung zum Löschen von Tags	Markieren	brokers		
			configurations		
				aws:TagKeys	
DeleteUser	Gewährt die Berechtigung zum Löschen eines ActiveMQ-Benutzers	Write	brokers*		
DescribeBroker	Gewährt die Berechtigung zum Zurückgeben von Informationen zum angegebenen Broker	Read	brokers*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeBrokerEngineTypes	Gewährt die Berechtigung, Informationen zu Broker-Engines zurückzugeben	Read			
DescribeBrokerInstanceOptions	Gewährt die Berechtigung, Informationen zu Broker-Instance-Optionen zurückzugeben	Read			
DescribeConfiguration	Gewährt die Berechtigung zum Zurückgeben von Informationen zur angegebenen Konfiguration	Read	configurations*		
DescribeConfigurationRevision	Gewährt die Berechtigung zum Zurückgeben der angegebenen Konfigurationsversion für die angegebene Konfiguration	Read	configurations*		
DescribeUser	Gewährt die Berechtigung zum Zurückgeben von Informationen zu einem ActiveMQ-Benutzer	Read	brokers*		
ListBrokers	Gewährt die Berechtigung zum Zurückgeben einer Liste aller Broker	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListConfigurationRevisions	Gewährt die Berechtigung zum Zurückgeben einer Liste aller vorhandenen Versionen für die angegebene Konfiguration	List	configurations*		
ListConfigurations	Gewährt die Berechtigung zum Zurückgeben einer Liste aller Konfigurationen	List			
ListTags	Gewährt die Berechtigung, eine Liste von Tags zurückzugeben	List	brokers configurations		
ListUsers	Gewährt die Berechtigung zum Zurückgeben einer Liste aller ActiveMQ-Benutzer	Auflisten	brokers*		
Promote	Gewährt die Berechtigung zum Heraufstufen eines Brokers	Schreiben	brokers*		
RebootBroker	Gewährt die Berechtigung, einen Broker neu zu starten	Write	brokers*		
UpdateBroker	Gewährt die Berechtigung zum Hinzufügen einer ausstehenden Konfigurationsänderung zu einem Broker	Write	brokers*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateConfiguration	Gewährt die Berechtigung zum Aktualisieren der angegebenen Konfiguration	Write	configurations*		
UpdateUser	Gewährt die Berechtigung zum Aktualisieren der Informationen zu einem ActiveMQ-Benutzer	Write	brokers*		

Von Amazon MQ definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
brokers	`arn:${Partition}:mq:${Region}:${Account}:broker:${BrokerName}:${BrokerId}`	aws:ResourceTag/${TagKey}
configurations	`arn:${Partition}:mq:${Region}:${Account}:configuration:${ConfigurationId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon MQ

Amazon MQ definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Neptune

Amazon Neptune (Servicepräfix: `neptune-db`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Neptune definierte Aktionen

- Von Amazon Neptune definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Neptune

Von Amazon Neptune definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelLoaderJob	Erteilung der Berechtigung zum Abbrechen eines Laderauftrags	Schreiben	database*		
CancelMLDataProcessingJob	Erteilung der Berechtigung zum Abbrechen eines ML-Datenverarbeitungsauftrags	Schreiben	database*		
CancelMLModelTrainingJob	Erteilung der Berechtigung zum Abbrechen eines ML-Modell-Trainingsauftrags	Schreiben	database*		
CancelMLModelTransformJob	Erteilung der Berechtigung zum Abbrechen eines ML-Modelltransformationsauftrags	Schreiben	database*		
CancelQuery	Erteilung der Berechtigung zum Abbrechen einer Abfrage	Schreiben	database*		
CreateMLEndpoint	Erteilung der Berechtigung zum Erstellen eines ML-Endpunkts	Schreiben	database*		
DeleteDataViaQuery	Erteilung der Berechtigung, Daten über Abfrage-APIs in der Datenbank zu löschen	Schreiben	database*		
				neptune-db:QueryLanguage	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteMLEndpoint	Erteilung der Berechtigung zum Löschen eines ML-Endpunkts	Schreiben	database*		
DeleteStatistics	Erteilung der Berechtigung zum Löschen aller Statistiken in der Datenbank	Schreiben	database*		
GetEngineStatus	Erteilung der Berechtigung zur Überprüfung des Status der Neptun-Engine	Lesen	database*		
GetGraphSummary	Gewährt die Berechtigung zum Abrufen der Diagrammübersicht aus der Datenbank	Lesen	database*		
GetLoaderJobStatus	Erteilung der Berechtigung zur Überprüfung des Status eines Ladevorgangs	Lesen	database*		
GetMLDataProcessingJobStatus	Erteilung der Berechtigung zur Überprüfung des Status eines ML-Datenverarbeitungsauftrags	Lesen	database*		
GetMLEndpointStatus	Erteilung der Berechtigung zur Überprüfung des Status eines ML-Endpunkts	Lesen	database*		
GetMLModelTrainingJobStatus	Erteilung der Berechtigung zur Überprüfung des Status eines ML-Modell-Trainingsauftrags	Lesen	database*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetMLModelTransformJobStatus	Erteilung der Berechtigung zur Überprüfung des Status eines ML-Modell-Transformationsauftrags	Lesen	database*		
GetQueryStatus	Erteilung der Berechtigung zur Überprüfung des Status aller aktiven Abfragen	Lesen	database*		
				neptune-db:QueryLanguage	
GetStatisticsStatus	Erteilung der Berechtigung zur Überprüfung des Statistikstatus der Datenbank	Lesen	database*		
GetStreamRecords	Erteilung der Berechtigung zum Abrufen von Stream-Aufzeichnungen von Neptune	Lesen	database*		
				neptune-db:QueryLanguage	
ListLoaderJobs	Ermöglicht die Auflistung aller Laderaufträge	Auflisten	database*		
ListMLDataProcessingJobs	Erteilung der Berechtigung zur Auflistung aller ML-Datenverarbeitungsaufträge	Auflisten	database*		
ListMLEndpoints	Erteilung der Berechtigung, alle ML-Endpunkte aufzulisten	Auflisten	database*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListMLModelTrainingJobs	Erteilung der Berechtigung, alle ML-Modell-Trainingsaufträge aufzulisten	Auflisten	database*		
ListMLModelTransformJobs	Erteilung der Berechtigung zur Auflistung aller ML-Modelltransformationsaufträge	Auflisten	database*		
ManageStatistics	Erteilung der Berechtigung zur Verwaltung von Statistiken in der Datenbank	Schreiben	database*		
ReadDataViaQuery	Erteilung der Berechtigung, Daten über Abfrage-APIs in der Datenbank zu lesen	Lesen	database*		
				neptune-db:QueryLanguage	
ResetDatabase	Erteilung der Berechtigung zum Abrufen des für das Zurücksetzen erforderlichen Tokens und Zurücksetzen der Neptune-Datenbank	Schreiben	database*		
StartLoaderJob	Erteilung der Berechtigung zum Starten eines Ladevorgangs	Schreiben	database*		
StartMLDataProcessingJob	Erteilung der Berechtigung zum Starten eines ML-Datenverarbeitungsauftrags	Schreiben	database*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartMLModelTrainingJob	Erteilung der Berechtigung zum Start eines ML-Modell-Trainingsauftrags	Schreiben	database*		
StartMLModelTransformJob	Erteilung der Berechtigung zum Starten eines ML-Modell transformationsauftrags	Schreiben	database*		
WriteDataViaQuery	Erteilung der Berechtigung, Daten über Abfrage-APIs in die Datenbank zu schreiben	Schreiben	database*		
				neptune-db:QueryLanguage	
connect	Gewährt Berechtigung für alle Datenzugriffsaktionen in Engine-Versionen vor 1.2.0.0	Schreiben	database*		

Von Amazon Neptune definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
database	`arn:${Partition}:neptune-db:${Region}:${Account}:${ClusterResourceId}/*`	

Bedingungsschlüssel für Amazon Neptune

Amazon Neptune definiert die folgenden Bedingungsschlüssel, die in einem `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
neptune-db:QueryLanguage	Filterung des Zugriffs nach Graphenmodell	String

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Neptune Analytics

Amazon Neptune Analytics (Servicepräfix: `neptune-graph`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Neptune Analytics definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

> **Note**
>
> Alle IAM-Aktionen außer 'ReadDataViaQuery', 'WriteDataViaQuery' und 'DeleteDataViaQuery' haben eine entsprechende API-Operation

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelImportTask	Gewährt die Berechtigung zum Abbrechen eines laufenden Importauftrags	Schreiben	import-task*		
CancelQuery	Erteilung der Berechtigung zum Abbrechen einer Abfrage	Schreiben	graph*		
				aws:ResourceTag/${TagKey}	
CreateGraph	Gewährt die Berechtigung zum Erstellen eines neuen Diagramms	Schreiben	graph*		iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					kms:DescribeKey
				aws:RequestTag/${TagKey} aws:TagKeys neptune-graph:PublicConnectivity	
CreateGraphSnapshot	Gewährt die Berechtigung zum Erstellen eines neuen Snapshots aus einem vorhandenen Diagramm	Schreiben	graph*		
			graph-snapshot		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateGraphUsingImportTask	Gewährt die Berechtigung zum Erstellen eines neuen Diagramms beim Importieren von Daten in das neue Diagramm	Schreiben	import-task*		iam:CreateServiceLinkedRole iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey
			graph		
				aws:RequestTag/${TagKey} aws:TagKeys neptune-graph:PublicConnectivity	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreatePrivateGraphEndpoint	Gewährt die Berechtigung zum Erstellen eines neuen privaten Diagramm-Endpunkts für den Zugriff auf das Diagramm von einer VPC aus	Schreiben	graph*		ec2:CreateVpcEndpoint ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint route53:AssociateV

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					PCWithHostedZone
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteDataViaQuery	Gewährt die Berechtigung zum Löschen von Daten über Abfrage-APIs im Diagramm	Schreiben	graph*		
				aws:ResourceTag/${TagKey}	
DeleteGraph	Gewährt die Berechtigung zum Löschen eines Diagramms	Schreiben	graph*		
				aws:ResourceTag/${TagKey}	
DeleteGraphSnapshot	Gewährt die Berechtigung zum Löschen eines Snapshots	Schreiben	graph-snapshot*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeletePrivateGraphEndpoint	Gewährt die Berechtigung zum Löschen eines privaten Diagramm-Endpunkts eines Diagramms	Schreiben	graph*		ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint route53:Disassocia

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					teVPCFromHostedZone
				aws:ResourceTag/${TagKey}	
GetEngineStatus	Gewährt die Berechtigung zur Überprüfung des Diagrammstatus	Lesen	graph*		
				aws:ResourceTag/${TagKey}	
GetGraph	Gewährt die Berechtigung zum Abrufen von Details zu einem Diagramm	Lesen	graph*		
				aws:ResourceTag/${TagKey}	
GetGraphSnapshot	Gewährt die Berechtigung zum Abrufen von Details zu einem Snapshot	Lesen	graph-snapshot*		
				aws:ResourceTag/${TagKey}	
GetGraphSummary	Gewährt die Berechtigung zum Abrufen der Daten im Diagramm	Lesen	graph*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetImportTask	Gewährt die Berechtigung zum Abrufen von Details über eine Importaufgabe	Lesen	import-task*		
GetPrivateGraphEndpoint	Gewährt die Berechtigung zum Abrufen von Details zu einem privaten Diagramm-Endpunkt eines Diagramms	Lesen	graph*		
				aws:ResourceTag/${TagKey}	
GetQueryStatus	Gewährt die Berechtigung zur Überprüfung des Status einer bestimmten Abfragen	Lesen	graph*		
				aws:ResourceTag/${TagKey}	
GetStatisticsStatus	Gewährt die Berechtigung zum Abrufen der Statistiken für die Daten im Diagramm	Lesen	graph*		
				aws:ResourceTag/${TagKey}	
ListGraphSnapshots	Gewährt die Berechtigung zum Auflisten der Snapshots in Ihrem Konto	Lesen	graph-snapshot*		
ListGraphs	Gewährt die Berechtigung zum Auflisten der Diagramme in Ihrem Konto	Lesen	graph*		
ListImportTasks	Gewährt die Berechtigung zum Auflisten der Portfolios in Ihrem Konto	Lesen	import-task*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListPrivateGraphEndpoints	Gewährt die Berechtigung zum Auflisten der privaten Diagramm-Endpunkte für ein bestimmtes Diagramm	Lesen	graph*		
				aws:ResourceTag/${TagKey}	
ListQueries	Erteilung der Berechtigung zur Überprüfung des Status aller aktiven Abfragen	Lesen	graph*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Neptune Analytics-Ressource	Lesen	graph		
			graph-snapshot		
				aws:ResourceTag/${TagKey}	
ReadDataViaQuery	Gewährt die Berechtigung zum Lesen von Daten über Abfrage-APIs im Diagramm	Lesen	graph*		
				aws:ResourceTag/${TagKey}	
ResetGraph	Gewährt die Berechtigung zum Zurücksetzen eines Diagramms, wodurch alle Daten im Diagramm gelöscht werden	Schreiben	graph*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RestoreGraphFromSnapshot	Gewährt die Berechtigung zum Erstellen eines neuen Diagramms aus einem vorhandenen Snapshot	Schreiben	graph-snapshot*		kms:CreateGrant kms:Decrypt kms:DescribeKey
			graph		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys neptune-graph:PublicConnectivity	
StartImportTask	Erteilt die Erlaubnis, Daten in ein vorhandenes Diagramm zu importieren	Schreiben	graph*		iam:PassRole
TagResource		Tagging	graph		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Gewährt die Berechtigung zum Markieren einer Neptune Analytics-Ressource		graph-snapshot		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Neptune Analytics-Ressource	Tagging	graph		
			graph-snapshot		
				aws:TagKeys	
UpdateGraph	Gewährt die Berechtigung zum Ändern eines Diagramms	Schreiben	graph*		
				aws:ResourceTag/${TagKey} neptune-graph:PublicConnectivity	
WriteDataViaQuery	Gewährt die Berechtigung zum Schreiben von Daten über Abfrage-APIs im Diagramm	Schreiben	graph*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	

Von Amazon Neptune Analytics definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
graph	`arn:${Partition}:neptune-graph:${Region}:${Account}:graph/${ResourceId}`	aws:ResourceTag/${TagKey}
graph-snapshot	`arn:${Partition}:neptune-graph:${Region}:${Account}:graph-snapshot/${ResourceId}`	aws:ResourceTag/${TagKey}
import-task	`arn:${Partition}:neptune-graph:${Region}:${Account}:import-task/${ResourceId}`	

Bedingungsschlüssel für Amazon Neptune Analytics

Amazon Neptune Analytics definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die

Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Schlüssel eines Tags und den Wert einer Anforderung	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	String
aws:TagKeys	Filtert den Zugriff nach den Tag-Schlüsseln in einer Anforderung	ArrayOfString
neptune-graph:PublicConnectivity	Filtert den Zugriff nach dem Wert des öffentlichen Konnektivitätsparameters, der in der Anfrage angegeben ist, oder nach seinem Standardwert, falls dieser nicht angegeben ist. Der gesamte Zugriff auf Graphen ist IAM-authentifiziert	Bool

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Network Firewall

AWS Network Firewall (Servicepräfix: `network-firewall`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Network Firewall definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWSzu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateFirewallPolicy	Gewährt die Berechtigung zum Erstellen einer Verknüpfung zwischen einer Firewall-Richtlinie und einer Firewall	Write	Firewall*		
			FirewallPolicy*		
AssociateSubnets	Gewährt die Berechtigung, Virtual-Private-Cloud(VPC)-Subnetze einer Firewall zuzuordnen	Schreiben	Firewall*		
CreateFirewall	Gewährt die Berechtigung zum Erstellen einer AWS Network Firewall-Firewall	Schreiben	Firewall*		iam:CreateServiceLinkedRole
			FirewallPolicy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFirewallPolicy	Gewährt die Berechtigung zum Erstellen einer Firewall-Richtlinie für AWS Network Firewall	Schreiben	FirewallPolicy*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleGroup	Gewährt die Berechtigung zum Erstellen einer AWS Network Firewall-Regelgruppe	Schreiben	StatefulRuleGroup		
			StatelessRuleGroup		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTLSInspectionConfiguration	Gewährt die Berechtigung zum Erstellen einer TLS-Inspektionskonfiguration für AWS Network Firewall	Schreiben	TLSInspectionConfiguration*		iam:CreateServiceLinkedRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFirewall	Gewährt die Berechtigung zum Löschen einer Firewall	Write	Firewall*		
DeleteFirewallPolicy	Gewährt die Berechtigung zum Löschen einer Firewall-Richtlinie	Write	FirewallPolicy*		
DeleteResourcePolicy	Gewährt die Berechtigung zum Löschen einer Ressourcenrichtlinie für eine Firewall-Richtlinie oder Regelgruppe	Write	FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		
DeleteRuleGroup	Gewährt die Berechtigung zum Löschen einer Regelgruppe	Schreiben	StatefulRuleGroup*		
			StatelessRuleGroup*		
DeleteTLSInspectionConfiguration	Gewährt die Berechtigung zum Löschen einer TLS-Inspektionskonfiguration	Schreiben	TLSInspectionConfiguration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeFirewall	Gewährt die Berechtigung zum Abrufen der Datenobjekte, die eine Firewall definieren	Read	Firewall*		
DescribeFirewallPolicy	Gewährt die Berechtigung zum Abrufen der Datenobjekte, die eine Firewall-Richtlinie definieren	Read	FirewallPolicy*		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
DescribeLoggingConfiguration	Gewährt die Berechtigung zum Beschreiben der Protokollierungskonfiguration einer Firewall	Read	Firewall*		
DescribeResourcePolicy	Gewährt die Berechtigung zum Beschreiben einer Ressourcenrichtlinie für eine Firewall-Richtlinie oder Regelgruppe	Read	FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeRuleGroup	Gewährt die Berechtigung zum Abrufen der Datenobjekte, die eine Regelgruppe definieren	Lesen	StatefulRuleGroup		
			StatelessRuleGroup		
DescribeRuleGroupMetadata	Gewährt die Berechtigung zum Abrufen von High-Level-Informationen für eine Regelgruppe	Lesen	StatefulRuleGroup		
			StatelessRuleGroup		
DescribeTLSInspectionConfiguration	Gewährt die Berechtigung zum Abrufen der Datenobjekte, die eine TLS-Inspektionskonfiguration definieren	Lesen	TLSInspectionConfiguration*		
DisassociateSubnets	Gewährt die Berechtigung, die Mapping von VPC-Subnetzen zu einer Firewall zu trennen	Write	Firewall*		
ListFirewallPolicies	Gewährt die Berechtigung zum Abrufen der Metadaten für Firewall-Richtlinien	List	FirewallPolicy*		
ListFirewalls	Gewährt die Berechtigung zum Abrufen der Metadaten für Firewalls	List	Firewall*		
ListRuleGroups	Gewährt die Berechtigung zum Abrufen der Metadaten für Regelgruppen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTLSInspectionConfigurations	Gewährt die Berechtigung zum Abrufen der Metadaten für TLS-Inspektionskonfigurationen	Auflisten	TLSInspectionConfiguration*		
ListTagsForResource	Gewährt die Berechtigung zum Abrufen der Tags für eine Ressource	List	Firewall*		
			FirewallPolicy*		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
PutResourcePolicy	Gewährt die Berechtigung zum Festlegen einer Ressourcenrichtlinie für eine Firewall-Richtlinie oder Regelgruppe	Write	FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		
TagResource	Gewährt die Berechtigung zum Anfügen von Tags an eine Ressource	Markieren	Firewall		
			FirewallPolicy		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Ressource	Markieren	Firewall		
			FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateFirewallDeleteProtection	Gewährt die Berechtigung zum Hinzufügen oder Entfernen des Löschungsschutzes einer Firewall	Write	Firewall*		
UpdateFirewallDescription	Gewährt die Berechtigung zum Ändern der Beschreibung für eine Firewall	Schreiben	Firewall*		
UpdateFirewallEncryptionConfiguration	Gewährt die Berechtigung zum Ändern der Protokollierungskonfiguration einer Firewall	Schreiben	Firewall*		
UpdateFirewallPolicy	Gewährt die Berechtigung zum Ändern einer Firewall-Richtlinie	Write	FirewallPolicy*		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
UpdateFirewallPolicyChangeProtection	Gewährt die Berechtigung zum Hinzufügen oder Entfernen von Änderungsschutz für die Firewall-Richtlinie einer Firewall	Write	Firewall*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateLoggingConfiguration	Gewährt die Berechtigung zum Ändern der Protokollierungskonfiguration einer Firewall	Write	Firewall*		
UpdateRuleGroup	Gewährt die Berechtigung zum Ändern einer Regelgruppe	Write	StatefulRuleGroup		
			StatelessRuleGroup		
UpdateSubnetChangeProtection	Gewährt die Berechtigung zum Hinzufügen oder Entfernen von Änderungsschutz für Subnetze für eine Firewall	Schreiben	Firewall*		
UpdateTLSInspectionConfiguration	Gewährt die Berechtigung zum Ändern einer TLS-Inspektionskonfiguration	Schreiben	TLSInspectionConfiguration*		

Von AWS Network Firewall definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Firewall	`arn:${Partition}:network-firewall:${Region}:${Account}:firewall/${Name}`	aws:ResourceTag/${TagKey}
FirewallPolicy	`arn:${Partition}:network-firewall:${Region}:${Account}:firewall-policy/${Name}`	aws:ResourceTag/${TagKey}
StatefulRuleGroup	`arn:${Partition}:network-firewall:${Region}:${Account}:stateful-rulegroup/${Name}`	aws:ResourceTag/${TagKey}
StatelessRuleGroup	`arn:${Partition}:network-firewall:${Region}:${Account}:stateless-rulegroup/${Name}`	aws:ResourceTag/${TagKey}
TLSInspectionConfiguration	`arn:${Partition}:network-firewall:${Region}:${Account}:tls-configuration/${Name}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Network Firewall

AWS Network Firewall definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den zulässigen Werten für jeden der Tags	String

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Tag-Wert, der der Ressource zugeordnet ist	String
aws:TagKeys	Filtert den Zugriff nach dem Vorhandensein verbindlicher Tags in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Network Manager

AWS Network Manager (Servicepräfix: `networkmanager`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Network Manager definierte Aktionen
- Von AWS Network Manager definierte Ressourcentypen
- Bedingungsschlüssel für AWS Network Manager

Von AWS Network Manager definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptAttachment	Gewährt die Berechtigung, die Erstellung einer Anlage zwischen einer Quelle und	Schreiben	attachment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	einem Ziel in einem Kernnetzwerk zu akzeptieren				
Associate ConnectPeer	Gewährt die Berechtigung zum Zuordnen eines Connect-Peers	Schreiben	device*		
			global-network*		
Associate CustomerGateway	Gewährt die Berechtigung, ein Kunden-Gateway mit einem Gerät zu verbinden	Write	device*		
			global-network*		
			link		
				networkmanager:cgwArn	
Associate Link	Gewährt die Berechtigung, einen Link mit einem Gerät zu verbinden	Write	device*		
			global-network*		
			link*		
Associate TransitGatewayConnectPeer	Gewährt die Berechtigung, einen Transit-Gateway-Connect-Peer einem Gerät zuzuordnen	Schreiben	device*		
			global-network*		
			link		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				networkmanager:tgwConnectPeerArn	
CreateConnectAttachment	Gewährt die Berechtigung zum Erstellen eines Connect-Anhangs	Schreiben	attachment*		
			core-network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnectPeer	Gewährt die Berechtigung zum Erstellen einer Connect-Peer-Verbindung	Schreiben	attachment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnection	Gewährt die Berechtigung zum Erstellen einer neuen Verbindung	Schreiben	global-network*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCoreNetwork	Gewährt die Berechtigung zum Erstellen eines neuen Kern-Netzwerks	Schreiben	global-network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDevice	Gewährt die Berechtigung zum Erstellen eines neuen Geräts	Write	global-network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateGlobalNetwork	Gewährt die Berechtigung zum Erstellen eines neuen globalen Netzwerks	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateLink	Gewährt die Berechtigung zum Erstellen eines neues Link.	Write	global-network*		
			site		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSite	Gewährt die Berechtigung zum Erstellen einer neuen Site.	Schreiben	global-network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSiteToSiteVpnAttachment	Gewährt die Berechtigung zum Erstellen eines Site-to-Site-VPN-Anhangs	Schreiben	core-network*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:vpnConnectionArn	
CreateTransitGatewayPeering	Gewährt die Berechtigung zum Erstellen eines Transit-Gateways	Schreiben	core-network*		
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:tgwArn	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTransitGatewayRouteTableAttachment	Gewährt die Berechtigung zum Erstellen eines VPC-Anhangs	Schreiben	peering*		
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:tgwRtbArn	
CreateVpcAttachment	Gewährt die Berechtigung zum Erstellen eines VPC-Anhangs	Schreiben	core-network*		
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:vpcArn networkmanager:subnetArns	
DeleteAttachment	Gewährt die Berechtigung zum Löschen eines Anhangs	Schreiben	attachment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteConnectPeer	Gewährt die Berechtigung zum Löschen eines Connect-Peers	Schreiben	connect-peer*		
DeleteConnection	Gewährt die Berechtigung zum Löschen einer Verbindung.	Schreiben	connection*		
			global-network*		
DeleteCoreNetwork	Gewährt die Berechtigung zum Löschen eines Kern-Netzwerks	Schreiben	core-network*		
DeleteCoreNetworkPolicyVersion	Gewährt die Berechtigung zum Löschen der Richtlinienversion eines Kern-Netzwerks	Schreiben	core-network*		
DeleteDevice	Gewährt die Berechtigung zum Löschen eines Geräts	Write	device*		
			global-network*		
DeleteGlobalNetwork	Gewährt die Berechtigung zum Löschen eines globalen Netzwerks	Write	global-network*		
DeleteLink	Gewährt die Berechtigung zum Löschen eines Links	Schreiben	global-network*		
			link*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeletePeering	Gewährt die Berechtigung zum Löschen eines Connect-Peers	Schreiben	peering*		
DeleteResourcePolicy	Gewährt die Berechtigung zum Löschen einer Ressource	Schreiben	core-network*		
DeleteSite	Gewährt die Berechtigung zum Löschen einer Website	Write	global-network*		
			site*		
DeregisterTransitGateway	Gewährt die Berechtigung zur Deregistrierung eines Transit-Gateways aus einem globalen Netzwerk	Write	global-network*		
				networkmanager:tgwArn	
DescribeGlobalNetworks	Gewährt die Berechtigung zur Beschreibung globaler Netzwerke	Auflisten	global-network		
DisassociateConnectPeer	Gewährt die Berechtigung zum Trennen eines Connect-Peers	Schreiben	global-network*		
DisassociateCustomerGateway	Gewährt die Berechtigung, ein Kunden-Gateway von einem Gerät zu trennen	Write	global-network*		
				networkmanager:cgwArn	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateLink	Gewährt die Berechtigung, einen Link von einem Gerät zu trennen	Write	device*		
			global-network*		
			link*		
DisassociateTransitGatewayConnectPeer	Gewährt die Berechtigung, die Mapping eines Transit-Gateway-Connect-Peer zu einem Gerät aufzuheben	Schreiben	global-network*		
				networkmanager:tgwConnectPeerArn	
ExecuteCoreNetworkChangeSet	Gewährt die Berechtigung zum Anwenden von Änderungen auf das Kern-Netzwerk	Schreiben	core-network*		
GetConnectAttachment	Gewährt die Berechtigung zum Abrufen eines Connect-Anhangs	Lesen	attachment*		
GetConnectPeer	Gewährt die Berechtigung zum Abrufen eines Connect-Peers	Lesen	connect-peer*		
GetConnectPeerAssociations	Gewährt die Berechtigung zum Beschreiben von Connect-Peer-Zuordnungen	Lesen	global-network*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetConnections	Gewährt die Berechtigung zum Beschreiben von Verbindungen	Auflisten	global-network*		
			connection		
GetCoreNetwork	Gewährt die Berechtigung zum Abrufen eines Kern-Netzwerks	Lesen	core-network*		
GetCoreNetworkChangeEvents	Gewährt die Berechtigung zum Abrufen einer Liste der Kern-Netzwerk-Änderungssätze	Lesen	core-network*		
GetCoreNetworkChangeSet	Gewährt die Berechtigung zum Abrufen einer Liste der Kern-Netzwerk-Änderungssätze	Lesen	core-network*		
GetCoreNetworkPolicy	Gewährt die Berechtigung zum Abrufen von Kern-Netzwerk-Richtlinien	Lesen	core-network*		
GetCustomerGatewayAssociations	Gewährt die Berechtigung, Kunden-Gateway-Mappings zu beschreiben	List	global-network*		
GetDevices	Gewährt die Berechtigung, Geräte zu beschreiben	List	global-network*		
			device		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetLinkAssociations	Gewährt die Berechtigung, Link-Verknüpfungen zu beschreiben	List	global-network*		
			device		
			link		
GetLinks	Gewährt die Berechtigung, Links zu beschreiben	Auflisten	global-network*		
			link		
GetNetworkResourceCounts	Gewährt die Berechtigung zum Zurückgeben der Anzahl der Ressourcen für ein globales Netzwerk, das nach Typ gruppiert ist	Lesen	global-network*		
GetNetworkResourceRelationships	Gewährt die Berechtigung zum Abrufen verwandter Ressourcen für eine Ressource innerhalb des globalen Netzwerks	Lesen	global-network*		
GetNetworkResources	Gewährt die Berechtigung zum Abrufen einer globalen Netzwerkressource	Lesen	global-network*		
GetNetworkRoutes	Gewährt die Berechtigung zum Abrufen von Routen für eine Routing-Tabelle innerhalb des globalen Netzwerks	Lesen	global-network*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetNetworkTelemetry	Gewährt die Berechtigung zum Abrufen von Netzwerk-Telemetrieobjekten für das globale Netzwerk	Lesen	global-network*		
GetResourcePolicy	Gewährt die Berechtigung zum Abrufen einer Ressourcenrichtlinie.	Lesen	core-network*		
GetRouteAnalysis	Gewährt die Berechtigung zum Abrufen einer Routenanalyse-Konfiguration und eines Ergebnisses	Lesen	global-network*		
GetSiteToSiteVpnAttachment	Gewährt die Berechtigung zum Abrufen eines Site-to-Site-VPN-Anhangs	Lesen	attachment*		
GetSites	Gewährt die Berechtigung zur Beschreibung globaler Netzwerke	List	global-network*		
			site		
GetTransitGatewayConnectPeerAssociations	Gewährt die Berechtigung zum Beschreiben von Transit-Gateway-Connect-Peer-Mappings	Auflisten	global-network*		
GetTransitGatewayPeering	Gewährt die Berechtigung zum Abrufen eines Transit Gateway	Lesen	peering*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetTransitGatewayRegistrations	Gewährt die Berechtigung, Transit-Gateway-Registrierungen zu beschreiben	Auflisten	global-network*		
GetTransitGatewayRouteTableAttachment	Gewährt die Berechtigung zum Abrufen eines VPC-Anhangs	Lesen	attachment*		
GetVpcAttachment	Gewährt die Berechtigung zum Abrufen eines VPC-Anhangs	Lesen	attachment*		
ListAttachments	Erteilt die Berechtigung zum Beschreiben eines Anhangs	Auflisten	attachment*		
ListConnectPeers	Gewährt die Berechtigung zum Beschreiben von Connect-Peers	Auflisten	connect-peer*		
ListCoreNetworkPolicyVersions	Gewährt die Berechtigung zum Auflisten von Netzwerk-Richtlinienversionen	Auflisten	core-network*		
ListCoreNetworks	Gewährt die Berechtigung zum Auflisten von Kern-Netzwerken	Auflisten			
ListOrganizationServiceAccessStatus	Erteilt die Berechtigung, den Zugriffsstatus des Organisationsservices aufzulisten	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListPeerings	Gewährt die Berechtigung zum Beschreiben von Verbindungen	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Network Manager-Ressource	Lesen	attachment		
			connect-peer		
			connection		
			core-network		
			device		
			global-network		
			link		
			peering		
			site		
				aws:ResourceTag/${TagKey}	
PutCoreNetworkPolicy	Gewährt die Berechtigung zum Erstellen einer neuen Kern-Netzwerk-Richtlinie	Schreiben	core-network*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutResourcePolicy	Gewährt die Berechtigung zum Erstellen oder Aktualisieren einer Ressourcenrichtlinie	Schreiben	core-network*		
RegisterTransitGateway	Gewährt die Berechtigung, ein Transit-Gateway in einem globalen Netzwerk zu registrieren	Schreiben	global-network*		
				networkmanager:tgwArn	
RejectAttachment	Gewährt die Berechtigung zum Ablehnen von Anhangs-Anforderungen	Schreiben	attachment*		
RestoreCoreNetworkPolicyVersion	Gewährt die Berechtigung zum Wiederherstellen der Kern-Netzwerk-Richtlinie auf eine frühere Version	Schreiben	core-network*		
StartOrganizationServiceAccessUpdate	Erteilt die Berechtigung, die Aktualisierung des Organisationsservicezugriffs zu starten	Schreiben			
StartRouteAnalysis	Gewährt die Berechtigung zum Starten einer Routenanalyse und speichert die Analysekonfiguration	Schreiben	global-network*		
TagResource	Gewährt die Berechtigung zum Markieren einer Network Manager-Ressource	Markieren	attachment		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			connect-peer		
			connection		
			core-network		
			device		
			global-network		
			link		
			peering		
			site		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Gewährt die Berechtigung, die Markierung einer Network Manager-Ressource aufzuheben	Markieren	attachment		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			connect-peer		
			connection		
			core-network		
			device		
			global-network		
			link		
			peering		
			site		
				aws:TagKeys	
UpdateConnection	Gewährt die Berechtigung zum Aktualisieren einer Verbindung.	Schreiben	connection*		
			global-network*		
UpdateCoreNetwork	Gewährt die Berechtigung zum Aktualisieren eines Kern-Netzwerks	Schreiben	core-network*		
UpdateDevice	Gewährt die Berechtigung, ein Gerät zu aktualisieren	Write	device*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			global-network*		
UpdateGlobalNetwork	Gewährt die Berechtigung, ein globales Netzwerk zu aktualisieren	Write	global-network*		
UpdateLink	Gewährt die Berechtigung, einen Link zu aktualisieren	Schreiben	global-network*		
			link*		
UpdateNetworkResourceMetadata	Gewährt die Berechtigung zum Hinzufügen oder Aktualisieren von Metadaten-Schlüssel-/Wert-Paaren auf der Netzwerkressource	Schreiben	global-network*		
UpdateSite	Gewährt die Berechtigung, eine Website zu aktualisieren	Schreiben	global-network*		
			site*		
UpdateVpcAttachment	Gewährt die Berechtigung zum Aktualisieren eines VPC-Anhangs	Schreiben	attachment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:subnetArns	

Von AWS Network Manager definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
global-network	`arn:${Partition}:networkmanager::${Account}:global-network/${ResourceId}`	aws:ResourceTag/${TagKey}
site	`arn:${Partition}:networkmanager::${Account}:site/${GlobalNetworkId}/${ResourceId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
link	`arn:${Partition}:networkmanager::${Account}:link/${GlobalNetworkId}/${ResourceId}`	aws:ResourceTag/${TagKey}
device	`arn:${Partition}:networkmanager::${Account}:device/${GlobalNetworkId}/${ResourceId}`	aws:ResourceTag/${TagKey}
connection	`arn:${Partition}:networkmanager::${Account}:connection/${GlobalNetworkId}/${ResourceId}`	aws:ResourceTag/${TagKey}
core-network	`arn:${Partition}:networkmanager::${Account}:core-network/${ResourceId}`	aws:ResourceTag/${TagKey}
attachment	`arn:${Partition}:networkmanager::${Account}:attachment/${ResourceId}`	aws:ResourceTag/${TagKey}
connect-peer	`arn:${Partition}:networkmanager::${Account}:connect-peer/${ResourceId}`	aws:ResourceTag/${TagKey}
peering	`arn:${Partition}:networkmanager::${Account}:peering/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Network Manager

AWS Network Manager definiert die folgenden Bedingungsschlüssel, die im -Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString
networkmanager:cgwArn	Filtert den Zugriff danach, welche Kunden-Gateways zugeordnet oder getrennt werden können	ARN
networkmanager:subnetArns	Filtert den Zugriff danach, welche VPC-Subnetze einem VPC-Anhang hinzugefügt oder entfernt werden können	ArrayOfARN
networkmanager:tgwArn	Filtert den Zugriff danach, welche Transit-Gateways an- oder abgemeldet werden können	ARN
networkmanager:tgwConnectPeerArn	Filtert den Zugriff danach, welche Transit-Gateway-Connect-Peers zugeordnet oder getrennt werden können	ARN
networkmanager:tgwRtbArn	Filtert den Zugriff, über den die Transit Gateway Gateway-Routentabelle zum Erstellen einer Anlage verwendet werden kann	ARN
networkmanager:vpcArn	Filtert den Zugriff danach, welches VPC zum Erstellen/Aktualisieren eines Anhangs verwendet werden kann	ARN
networkmanager:vpnConnectionArn	Filtert den Zugriff danach, welche Site-to-Site-VPN zum Erstellen/Aktualisieren eines Anhangs verwendet werden kann	ARN

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Network Manager Chat

AWS Network Manager Chat (Servicepräfix: `networkmanager-chat`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Network Manager Chat definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelMessageResponse [nur Berechtigung]	Gewährt die Berechtigung zum Abbrechen einer Antwort auf eine Nachricht	Schreiben			
CreateConversation [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer Konversation	Schreiben			
DeleteConversation [nur Berechtigung]	Gewährt die Berechtigung zum Löschen einer Konversation	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListConversationMessages [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Konversationsbenachrichtigungen	Auflisten			
ListConversations [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Konversationen	Auflisten			
NotifyConversationIsActive [nur Berechtigung]	Gewährt die Berechtigung über Aktivitäten in einem Gespräch	Schreiben			
SendConversationMessage [nur Berechtigung]	Gewährt die Berechtigung zum Senden einer Nachricht in einer Konversation als Unternehmen	Schreiben			

Von AWS Network Manager Chat definierte Ressourcentypen

AWS Network Manager Chat unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf AWS Network Manager Chat zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Network Manager Chat

Network Manager Chat besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Nimble Studio

Amazon Nimble Studio (Service-Präfix: `nimble`) bietet die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Nimble Studio definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptEulas	Gewährt die Berechtigung zum Annehmen von EULAs	Write	eula*		
CreateLaunchProfile	Gewährt die Berechtigung zum Erstellen eines Startprofils	Write	studio*		ec2:CreateNetworkInterface ec2:DescribeNatGateways ec2:DescribeNetworkAcls

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ec2:DescribeRouteTables ec2:DescribeSubnets ec2:DescribeVpcEndpoints ec2:RunInstances
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateStreamingImage	Gewährt die Berechtigung zum Erstellen eines Streaming-Images	Write	studio*		ec2:DescribeImages ec2:DescribeSnapshots ec2:ModifyInstanceAttribute ec2:ModifySnapshotAttribute ec2:RegisterImage
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateStreamingSession	Gewährt die Berechtigung zum Erstellen einer Streaming-Sitzung	Write	launch-profile*		ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission nimble:GetLaunchProfile nimble:GetLaunchProfileInitialization nimble:ListEulaAcceptances
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStreamingSessionStream	Gewährt die Berechtigung zum Erstellen eines Streaming SessionStream	Write	streaming-session*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				nimble:requesterPrincipalId	
CreateStudio	Gewährt die Berechtigung zum Erstellen eines Studios	Write	studio*		iam:PassRole sso:CreateManagedApplicationInstance
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateStudioComponent	Gewährt die Berechtigung zum Erstellen einer Studiokomponente. Eine Studio-Komponente bezeichnet eine Netzwerkressource, auf die ein Startprofil Zugriff gewährt	Write	studio*		ds:AuthorizeApplication ds:DescribeDirectories ec2:DescribeSecurityGroups fsx:DescribeFileSystems iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteLaunchProfile	Gewährt die Berechtigung zum Löschen eines Startprofils	Write	launch-profile*		
DeleteLaunchProfileMember	Gewährt die Berechtigung zum Löschen eines Startprofil-Mitglieds	Write	launch-profile*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteStreamingImage	Gewährt die Berechtigung zum Löschen eines Streaming-Images	Write	streaming-image*		ec2:DeleteSnapshot ec2:DeregisterImage ec2:ModifyInstanceAttribute ec2:ModifySnapshotAttribute
DeleteStreamingSession	Gewährt die Berechtigung zum Löschen einer Streaming-Sitzung	Write	streaming-session*		ec2:DeleteNetworkInterface
				nimble:requesterPrincipalId	
DeleteStudio	Gewährt die Berechtigung zum Löschen eines Studios	Write	studio*		sso:DeleteManagedApplicationInstance
DeleteStudioComponent	Gewährt die Berechtigung zum Löschen einer Studiokomponente	Write	studio-component*		ds:UnauthorizeApplication

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteStudioMember	Gewährt die Berechtigung zum Löschen eines Studio-Mitglieds	Write	studio*		
GetEula	Gewährt die Berechtigung zum Abrufen einer EULA	Read	eula*		
GetFeatureMap [nur Berechtigung]	Gewährt die Berechtigung, dem Nimble-Studio-Portal zu erlauben, die entsprechenden Funktionen für dieses Konto anzuzeigen	Read			
GetLaunchProfile	Gewährt die Berechtigung zum Abrufen eines Startprofils	Read	launch-profile*		
GetLaunchProfileDetails	Gewährt die Berechtigung zum Abrufen der Details eines Startprofils, einschließlich der Zusammenfassung der vom Startprofil verwendeten Studiokomponenten und Streaming-Images	Read	launch-profile*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetLaunchProfileInitialization	Gewährt die Berechtigung zum Abrufen einer Initialisierung des Startprofils. Eine Initialisierung des Startprofils ist eine dereferenzierte Version eines Startprofils, einschließlich angehängter Verbindungsinformationen für Studio-Komponenten	Read	launch-profile*		ds:DescribeDirectories ec2:DescribeSecurityGroups fsx:DescribeFileSystems
GetLaunchProfileMember	Gewährt die Berechtigung zum Abrufen eines Startprofil-Mitglieds	Read	launch-profile*		
GetStreamingImage	Gewährt die Berechtigung zum Abrufen eines Streaming-Images	Read	streaming-image*		
GetStreamingSession	Gewährt die Berechtigung zum Abrufen einer Streaming-Sitzung	Lesen	streaming-session*		
				nimble:requesterPrincipalId	
GetStreamingSessionBackup	Gewährt die Berechtigung zum Abrufen eines Streaming-Sitzungs-Backups	Lesen	streaming-session-backup*		
				nimble:requesterPrincipalId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetStreamingSessionStream	Gewährt die Berechtigung zum Abrufen eines Streams für eine Streaming-Sitzung	Read	streaming-session*		
				nimble:requesterPrincipalId	
GetStudio	Gewährt die Berechtigung zum Abrufen eines Studios	Read	studio*		
GetStudioComponent	Gewährt die Berechtigung zum Abrufen einer Studio-Komponente	Read	studio-component*		
GetStudioMember	Gewährt die Berechtigung zum Abrufen eines Studio-Mitglieds	Read	studio*		
ListEulaAcceptances	Gewährt die Berechtigung zum Auflisten von EULA-Annahmen	Read	eula-acceptance*		
ListEulas	Gewährt die Berechtigung zum Auflisten von EULAs	Read	eula*		
ListLaunchProfileMembers	Gewährt die Berechtigung zum Auflisten von Startprofil-Mitgliedern	Read	launch-profile*		
ListLaunchProfiles	Gewährt die Berechtigung zum Auflisten von Startprofilen	Read	studio*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				nimble:principalId nimble:requesterPrincipalId	
ListStreamingImages	Gewährt die Berechtigung zum Auflisten von Streaming-Images	Lesen	studio*		
ListStreamingSessionBackups	Gewährt die Berechtigung zum Auflisten von Streaming-Sitzungs-Backups	Lesen	studio*		
				nimble:requesterPrincipalId	
ListStreamingSessions	Gewährt die Berechtigung zum Auflisten von Streaming-Sitzungen	Read	studio*		
				nimble:createdBy nimble:ownedBy nimble:requesterPrincipalId	
ListStudioComponents	Gewährt Berechtigung zum Auflisten von Studio-Komponenten	Read	studio*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListStudioMembers	Gewährt die Berechtigungen zum Auflisten von Studio-Mitgliedern	Read	studio*		
ListStudios	Gewährt die Berechtigung zum Auflisten aller Studios	Read			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten aller Tags auf einer Nimble-Studio-Ressource	Read	launch-profile		
			streaming-image		
			streaming-session		
			streaming-session-backup		
			studio		
			studio-component		
PutLaunchProfileMembers	Gewährt die Berechtigung zum Hinzufügen/Aktualisieren von Startprofil-Mitgliedern	Write	launch-profile*		sso-directory:DescribeUsers

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutStudioLogEvents [nur Berechtigung]	Gewährt die Berechtigung zur Protokollierung von Metriken und Protokollen für das Nimble-Studio-Portal zur Überwachung des Anwendungszustands	Write	studio*		
PutStudioMembers	Gewährt die Berechtigung zum Hinzufügen/Aktualisieren von Studio-Mitgliedern	Schreiben	studio*		sso-directory:DescribeUsers
StartStreamingSession	Gewährt die Berechtigung zum Starten einer Streaming-Sitzung	Schreiben	streaming-session*		nimble:GetLaunchProfile nimble:GetLaunchProfileMember
			streaming-session-backup		
				nimble:requesterPrincipalId	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartStudioSSOConfigurationRepair	Erteilt die Berechtigung zur Reparatur der Konfiguration des AWS IAM Identity Center des Studios	Schreiben	studio*		sso:CreateManagedApplicationInstance sso:GetManagedApplicationInstance
StopStreamingSession	Gewährt die Berechtigung zum Stoppen einer Streaming-Sitzung	Schreiben	streaming-session*		nimble:GetLaunchProfile
				nimble:requesterPrincipalId	
TagResource	Gewährt die Berechtigung zum Hinzufügen oder Überschreiben von einem oder mehreren Tags für die angegebene Nimble-Studio-Ressource	Markieren	launch-profile		
			streaming-image		
			streaming-session		
			streaming-session-backup		
			studio		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			studio-component		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Mapping ein oder mehrerer Tags aus der angegebenen Nimble-Studio-Ressource	Markieren	launch-profile		
			streaming-image		
			streaming-session		
			streaming-session-backup		
			studio		
			studio-component		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateLaunchProfile	Gewährt die Berechtigung zum Aktualisieren eines Startprofils	Write	launch-profile*		ec2:DescribeNatGateways ec2:DescribeNetworkAcls ec2:DescribeRouteTables ec2:DescribeSubnets ec2:DescribeVpcEndpoints
UpdateLaunchProfileMember	Gewährt die Berechtigung zum Aktualisieren eines Startprofil-Mitglieds	Write	launch-profile*		
UpdateStreamingImage	Gewährt die Berechtigung zum Aktualisieren eines Streaming-Images	Write	streaming-image*		
UpdateStudio	Gewährt die Berechtigung zum Aktualisieren eines Studios	Write	studio*		iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateStudioComponent	Gewährt die Berechtigung zum Aktualisieren einer Studio-Komponente	Write	studio-component*		ds:AuthorizeApplication ds:DescribeDirectories ec2:DescribeSecurityGroups fsx:DescribeFileSystems iam:PassRole

Von Amazon Nimble Studio definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
studio	`arn:${Partition}:nimble:${Region}:${Account}:studio/${StudioId}`	aws:RequestTag/${TagKey}

Ressource ntypen	ARN	Bedingungsschlüssel
		aws:ResourceTag/${TagKey} aws:TagKeys nimble:studioId
streaming-image	arn:${Partition}:nimble:${Region}:${Account}:streaming-image/${StreamingImageId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:studioId
studio-component	arn:${Partition}:nimble:${Region}:${Account}:studio-component/${StudioComponentId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:studioId
launch-profile	arn:${Partition}:nimble:${Region}:${Account}:launch-profile/${LaunchProfileId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:studioId

Ressourcentypen	ARN	Bedingungsschlüssel
streaming-session	`arn:${Partition}:nimble:${Region}:${Account}:streaming-session/${StreamingSessionId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:createdBy nimble:ownedBy
streaming-session-backup	`arn:${Partition}:nimble:${Region}:${Account}:streaming-session-backup/${StreamingSessionBackupId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:ownedBy
eula	`arn:${Partition}:nimble:${Region}:${Account}:eula/${EulaId}`	
eula-acceptance	`arn:${Partition}:nimble:${Region}:${Account}:eula-acceptance/${EulaAcceptanceId}`	nimble:studioId

Bedingungsschlüssel für Amazon Nimble Studio

Amazon Nimble Studio definiert die folgenden Bedingungsschlüssel, die in einem `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wertepaaren, die in der Anforderung zulässig sind	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paar einer Ressource	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach Liste von Tag-Schlüsseln, die in der Anforderung zulässig sind	ArrayOfString
nimble:createdBy	Filtert den Zugriff basierend auf dem createdBy-Anforderungsparameter oder der ID des Erstellers der Ressource	Zeichenfolge
nimble:ownedBy	Filtert den Zugriff basierend auf dem ownedBy-Anforderungsparameter oder der ID des Besitzers der Ressource	Zeichenfolge
nimble:principalId	Filtert den Zugriff basierend auf dem Anforderungsparameter principalId	Zeichenfolge
nimble:requesterPrincipalId	Filtert den Zugriff nach ID des angemeldeten Benutzers	Zeichenfolge
nimble:studioId	Filtert den Zugriff nach einem bestimmten Studio	ARN

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon One Enterprise

Amazon One Enterprise (Servicepräfix: one) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon One Enterprise definierte Aktionen
- Von Amazon One Enterprise definierte Ressourcentypen
- Bedingungsschlüssel für Amazon One Enterprise

Von Amazon One Enterprise definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDeviceActivationQrCode	Gewährt die Berechtigung zum Erstellen eines QR-Codes für eine Geräte-Instance	Schreiben	device-instance*		
				aws:ResourceTag/${TagKey}	
CreateDeviceConfigurationTemplate	Gewährt die Berechtigung zum Erstellen einer Geräte-Konfigurationsvorlage	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeviceInstance	Gewährt die Berechtigung zum Erstellen einer Geräte-Instance	Schreiben		aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
CreateDeviceInstanceConfiguration	Gewährt die Berechtigung zum Erstellen einer Geräte-Instance-Konfiguration	Schreiben	device-instance*		
				aws:ResourceTag/${TagKey}	
CreateSite	Gewährt die Berechtigung zum Erstellen einer Site	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAssociatedDevice	Gewährt die Berechtigung, einen Link von einer Geräte-Instance zu trennen	Schreiben	device-instance*		
				aws:ResourceTag/${TagKey}	
DeleteDeviceConfigurationTemplate	Gewährt die Berechtigung zum Löschen einer Geräte-Konfigurationsvorlage	Schreiben	device-configuration-template*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteDeviceInstance	Gewährt die Berechtigung zum Löschen einer Geräte-Instance	Schreiben	device-instance*		
				aws:ResourceTag/${TagKey}	
DeleteSite	Gewährt die Berechtigung zum Löschen einer Website	Schreiben	site*		
				aws:ResourceTag/${TagKey}	
DeleteUser	Gewährt die Berechtigung zum Löschen eines Benutzers	Schreiben	user*		
GetDeviceConfigurationTemplate	Gewährt die Berechtigung zum Löschen einer Geräte-Konfigurationsvorlage	Lesen	device-configuration-template*		
				aws:ResourceTag/${TagKey}	
GetDeviceInstance	Gewährt die Berechtigung zum Anzeigen einer Geräte-Instance	Lesen	device-instance*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDeviceInstanceConfiguration	Gewährt die Berechtigung zum Anzeigen einer Geräte-Instance-Konfiguration	Lesen	configuration*		
				aws:ResourceTag/${TagKey}	
GetSite	Gewährt die Berechtigung zum Anzeigen einer Website	Lesen	site*		
				aws:ResourceTag/${TagKey}	
GetSiteAddress	Gewährt die Berechtigung zum Anzeigen einer Website	Lesen	site*		
				aws:ResourceTag/${TagKey}	
ListDeviceConfigurationTemplates	Gewährt die Berechtigung zum Abrufen der Liste von Gerätekonfigurationsvorlagen	Auflisten			
ListDeviceInstances	Gewährt die Berechtigung zum Abrufen einer Liste von Geräte-Instances	Auflisten			
ListSites	Gewährt die Berechtigung zum Auflisten von Websites	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Amazon One Enterprise-Ressourcen	Lesen	device-configuration-template		
			device-instance		
			site		
				aws:ResourceTag/${TagKey}	
ListUsers	Gewährt die Berechtigung zum Anzeigen der Liste von Benutzern	Auflisten			
RebootDevice	Gewährt die Berechtigung, das einer Geräte-Instance zugeordnete Gerät neu zu starten	Schreiben	device-instance*		
				aws:ResourceTag/${TagKey}	
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Amazon One Enterprise-Ressource	Markierung	device-configuration-template		
			device-instance		
			site		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Amazon One Enterprise-Ressource	Markierung	device-configuration-template		
			device-instance		
			site		
				aws:TagKeys	
UpdateDeviceConfigurationTemplate	Gewährt die Berechtigung zum Aktualisieren einer Gerätekonfigurationsvorlage	Schreiben	device-configuration-template*		
				aws:ResourceTag/${TagKey}	
UpdateDeviceInstance	Gewährt die Berechtigung, eine Gerät-Instance zu aktualisieren	Schreiben	device-instance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
UpdateSite	Gewährt die Berechtigung, eine Website zu aktualisieren	Schreiben	site*		
				aws:ResourceTag/${TagKey}	
UpdateSiteAddress	Gewährt die Berechtigung zum Aktualisieren der Website-Adresse	Schreiben	site*		
				aws:ResourceTag/${TagKey}	

Von Amazon One Enterprise definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
device-instance	`arn:${Partition}:one:${Region}:${Account}:device-instance/${DeviceInstanceId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
configuration	`arn:${Partition}:one:${Region}:${Account}:device-instance/${DeviceInstanceId}/configuration/${Version}`	
device-configuration-template	`arn:${Partition}:one:${Region}:${Account}:device-configuration-template/${TemplateId}`	aws:ResourceTag/${TagKey}
site	`arn:${Partition}:one:${Region}:${Account}:site/${SiteId}`	aws:ResourceTag/${TagKey}
user	`arn:${Partition}:one:${Region}:${Account}:user/${UserId}`	

Bedingungsschlüssel für Amazon One Enterprise

Amazon One Enterprise definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff mithilfe von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen mithilfe von Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon OpenSearch Ingestion

Amazon OpenSearch Ingestion (Servicepräfix: `osis`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon OpenSearch Ingestion definierte Aktionen
- Von Amazon OpenSearch Ingestion definierte Ressourcentypen
- Bedingungsschlüssel für Amazon OpenSearch Ingestion

Von Amazon OpenSearch Ingestion definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreatePipeline	Gewährt die Berechtigung zum Erstellen einer OpenSearch Aufnahme-Pipeline	Schreiben		aws:TagKeys	iam:CreateServiceLinkedRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey}	iam:PassRole kms:DescribeKey kms:GenerateDataKeyWithoutPlaintext logs:CreateLogDelivery
DeletePipeline	Gewährt die Berechtigung zum Löschen einer OpenSearch Aufnahme-Pipeline	Schreiben	pipeline*		logs:DeleteLogDelivery logs:GetLogDelivery logs:ListLogDeliveries
GetPipeline	Gewährt die Berechtigung zum Abrufen von Konfigurationsinformationen für eine OpenSearch Aufnahme-Pipeline	Lesen	pipeline*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetPipelineBlueprint	Gewährt die Berechtigung zum Abrufen des Inhalts eines OpenSearch Ingestion-Pipeline-Blueprints	Lesen	pipeline-blueprint*		
GetPipelineChangeProgress	Gewährt die Berechtigung zum Abrufen detaillierter Informationen über den Status einer OpenSearch Aufnahme-Pipeline	Lesen	pipeline*		
Ingest	Gewährt die Berechtigung zum Aufnehmen von Daten über eine OpenSearch Aufnahme-Pipeline	Schreiben	pipeline*		
ListPipelineBlueprints	Gewährt die Berechtigung zum Auflisten der Namen der verfügbaren Vorlagen für eine OpenSearch Ingestion-Pipeline-Konfiguration	Auflisten			
ListPipelines	Gewährt die Berechtigung zum Auflisten der Grundkonfiguration für jede OpenSearch Aufnahme-Pipeline im aktuellen Konto und in der Region	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Auflisten aller Ressourcen-Tags, die einer OpenSearch Aufnahme-Pipeline zugeordnet sind	Lesen	pipeline*		
StartPipeline	Gewährt die Berechtigung zum Starten einer OpenSearch Aufnahme-Pipeline	Schreiben	pipeline*		
StopPipeline	Gewährt die Berechtigung zum Stoppen einer OpenSearch Aufnahme-Pipeline	Schreiben	pipeline*		
TagResource	Gewährt die Berechtigung zum Anfügen von Ressourcen-Tags an eine OpenSearch Aufnahme-Pipeline	Tagging	pipeline*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Ressourcen-Tags aus einer OpenSearch Ingestion Service Pipeline	Tagging	pipeline*		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdatePipeline	Gewährt die Berechtigung zum Ändern der Konfiguration einer OpenSearch Aufnahme-Pipeline	Schreiben	pipeline*		iam:PassRole kms:DescribeKey kms:GenerateDataKeyWithoutPlaintext logs:GetLogDelivery logs:ListLogDeliveries logs:UpdateLogDelivery
ValidatePipeline	Gewährt die Berechtigung zum Überprüfen der Konfiguration einer OpenSearch Aufnahme-Pipeline	Lesen			

Von Amazon OpenSearch Ingestion definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können.

Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
pipeline	`arn:${Partition}:osis:${Region}:${Account}:pipeline/${PipelineName}`	aws:ResourceTag/${TagKey}
pipeline-blueprint	`arn:${Partition}:osis:${Region}:${Account}:blueprint/${BlueprintName}`	

Bedingungsschlüssel für Amazon OpenSearch Ingestion

Amazon OpenSearch Ingestion definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon OpenSearch Serverless

Amazon OpenSearch Serverless (Service-Präfix: `aoss`) bietet die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon OpenSearch Serverless definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
APIAccessAll	Gewährt die Berechtigung für alle unterstützten Opensearch-APIs	Schreiben	Collection*		
BatchGetCollection	Gewährt die Berechtigung zum Abrufen von Attributen für eine oder mehrere Sammlungen	Lesen			
BatchGetEffectiveLifecyclePolicy	Gewährt die Berechtigung zum Abrufen von Informationen über eine Lebenszyklusrichtlinie, die auf eine oder	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	mehrere AOSS-Ressourcen angewendet wird				
BatchGetLifecyclePolicy	Gewährt die Berechtigung zum Abrufen von Informationen zu einzelnen oder mehreren Lebenszyklusrichtlinien	Lesen			
BatchGetVpcEndpoint	Gewährt die Berechtigung zum Abrufen von Attributen für einen oder mehrere VPC-Endpunkte	Lesen			
CreateAccessPolicy	Gewährt die Berechtigung zum Erstellen einer Datenzugriffsrichtlinie	Schreiben		aoss:collection aoss:index	
CreateCollection	Gewährt die Berechtigung zum Erstellen einer Serverless-Sammlung	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLifecyclePolicy	Gewährt die Berechtigung zum Erstellen einer Lebenszyklusrichtlinie	Schreiben		aoss:collection aoss:index	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSecurityConfig	Gewährt die Berechtigung zum Erstellen einer Serverless-Sicherheitskonfiguration	Schreiben			
CreateSecurityPolicy	Gewährt die Berechtigung zum Erstellen einer Netzwerk- oder Verschlüsselungsrichtlinie	Schreiben		aoss:collection	
CreateVpcEndpoint	Gewährt die Berechtigung zum Erstellen eines von OpenSearch Serverless verwalteten VPC-Schnittstellenendpunkts	Schreiben			
DashboardsAccessAll	Gewährt die Berechtigung für Opensearch Serverless Dashboards	Schreiben	Dashboards*		
DeleteAccessPolicy	Gewährt die Berechtigung zum Löschen einer Daten-Zugriffsrichtlinie	Schreiben		aoss:collection aoss:index	
DeleteCollection	Gewährt die Berechtigung zum Löschen einer Serverless-Sammlung	Schreiben	Collection*		
DeleteLifecyclePolicy	Gewährt die Berechtigung zum Löschen einer Lebenszyklusrichtlinie	Schreiben		aoss:collection aoss:index	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteSecurityConfig	Gewährt die Berechtigung zum Löschen einer Sicherheitskonfiguration.	Schreiben			
DeleteSecurityPolicy	Gewährt die Berechtigung zum Löschen einer Sicherheitsrichtlinie	Schreiben		aoss:collection	
DeleteVpcEndpoint	Gewährt die Berechtigung zum Löschen eines von OpenSearch Serverless verwalteten Schnittstellen-VPC-Endpunkts	Schreiben			
GetAccessPolicy	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Daten-Zugriffsrichtlinie	Lesen		aoss:collection aoss:index	
GetAccountSettings	Gewährt die Berechtigung zum Abrufen von Kontoeinstellungen, einschließlich der Kapazitätseinstellungen	Lesen			
GetPoliciesStats	Gewährt die Berechtigung zum Abrufen von Statistiken zu den Sicherheitsrichtlinien in Ihrem Konto	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetSecurityConfig	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Serverless-Sicherheitskonfiguration	Lesen			
GetSecurityPolicy	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Sicherheitsrichtlinie	Lesen		aoss:collection	
ListAccessPolicies	Gewährt die Berechtigung zum Auflisten von Datenzugriffsrichtlinien	Auflisten			
ListCollections	Gewährt die Berechtigung zum Auflisten von Sammlungen	Auflisten			
ListLifecyclePolicies	Gewährt die Berechtigung zum Auflisten von Lebenszyklusrichtlinien	Auflisten			
ListSecurityConfigs	Gewährt die Berechtigung zum Auflisten von Sicherheitskonfigurationen	Auflisten			
ListSecurityPolicies	Gewährt die Berechtigung zum Auflisten von Sicherheitsrichtlinien	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Sammlung	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListVpcEndpoints	Gewährt die Berechtigung zum Auflisten von OpenSearch Serverless verwalteten VPC-Endpunkten	Auflisten			
TagResource	Gewährt die Berechtigung zum Kennzeichnen einer Serverless-Sammlung mit Tags	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Sammlung	Schreiben		aws:TagKeys	
UpdateAccessPolicy	Gewährt die Berechtigung zum Aktualisieren einer Daten-Zugriffsrichtlinie	Schreiben		aoss:collection aoss:index	
UpdateAccountSettings	Gewährt die Berechtigung zum Aktualisieren von Kontoeinstellungen einschließlich der Kapazitätseinstellungen	Schreiben			
UpdateCollection	Gewährt die Berechtigung zum Aktualisieren einer Sammlung	Schreiben	Collection*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateLifecyclePolicy	Gewährt die Berechtigung zum Aktualisieren einer Lebenszyklusrichtlinie	Schreiben		aoss:collection aoss:index	
UpdateSecurityConfig	Gewährt die Berechtigung zur Aktualisierung der Sicherheits-Konfiguration	Schreiben			
UpdateSecurityPolicy	Gewährt die Berechtigung zum Aktualisieren einer Sicherheitsrichtlinie	Schreiben		aoss:collection	
UpdateVpcEndpoint	Gewährt die Berechtigung zum Aktualiseren von OpenSearch Serverless verwalteten VPC-Endpunkten	Schreiben			

Von Amazon OpenSearch Serverless definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Collection	`arn:${Partition}:aoss:${Region}:${Account}:collection/${CollectionId}`	aws:ResourceTag/${TagKey}
Dashboards	`arn:${Partition}:aoss:${Region}:${Account}:dashboards/default`	

Bedingungsschlüssel für Amazon OpenSearch Serverless

Amazon OpenSearch Serverless definiert die folgenden Bedingungsschlüssel, die in einem `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aoss:CollectionId	Filtert den Zugriff nach der ID der Sammlung	Zeichenfolge
aoss:collection	Filtert den Zugriff nach dem Sammlungsnamen	Zeichenfolge
aoss:index	Filtert den Zugriff anhand des Index	Zeichenfolge
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüsseln, die in der Anforderung übergeben werden.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon OpenSearch Service

Amazon OpenSearch Service (Service-Präfix: `es`) bietet die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon OpenSearch Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptInboundConnection	Gewährt die Berechtigung für den Eigentümer der Ziel-Domain, eine eingehende clusterübergreifende Suchverbindungsanforderung zu akzeptieren	Schreiben			
AcceptInboundCrossClusterSearchConnection	Gewährt die Berechtigung für den Eigentümer der Ziel-Domain, eine eingehende clusterübergreifende Suchverbindungsanforderung zu akzeptieren Diese Berechtig	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	ung ist veraltet. Verwenden Sie stattdessen AcceptInboundConnection				
AddDataSource	Gewährt die Berechtigung zum Hinzufügen der Datenquelle für die OpenSearch-Service-Domain	Schreiben	domain*		
AddTags	Gewährt die Berechtigung zum Anfügen von Ressourcen-Tags an eine OpenSearch Service-Domain	Markierung	domain*		
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociatePackage	Gewährt die Berechtigung zum Zuordnen eines Pakets zu einer OpenSearch-Service-Domain	Schreiben	domain*		
AuthorizeVpcEndpointAccess	Gewährt die Berechtigung, über einen Schnittstellen-VPC-Endpunkt Zugriff auf eine Domain von Amazon OpenSearch Service zu gewähren	Schreiben			
CancelDomainConfigChange	Gewährt die Berechtigung zum Erstellen einer OpenSearch Service-Domain	Schreiben	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelElasticsearchServiceSoftwareUpdate	Gewährt die Erlaubnis zum Abbrechen des Updates einer Service-Software einer Domain. Diese Berechtigung ist veraltet. Verwenden Sie stattdessen CancelServiceSoftwareUpdate	Schreiben	domain*		
CancelServiceSoftwareUpdate	Gewährt die Erlaubnis zum Abbrechen des Updates einer Service-Software einer Domain	Schreiben	domain*		
CreateDomain	Gewährt die Berechtigung zum Erstellen einer Amazon OpenSearch Service-Domain	Schreiben	domain		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateElasticsearchDomain	Gewährt die Berechtigung zum Erstellen einer OpenSearch Service-Domain Diese Berechtigung ist veraltet. Verwenden Sie stattdessen CreateDomain	Schreiben	domain		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateElasticsearchServiceRole	Gewährt die Berechtigung zum Erstellen der serviceverknüpften Rolle, die für OpenSearch Service-Domains erfoderlich ist, die VPC-Zugriff nutzen. Diese Berechtigung ist veraltet. OpenSearch Service erstellt die serviceverknüpfte Rolle für Sie	Schreiben			
CreateOutboundConnection	Gewährt die Berechtigung zum Erstellen einer neuen clusterübergreifenden Suchverbindung von einer Quell-Domain zu einer Ziel-Domain	Schreiben	domain*		
CreateOutboundCrossClusterSearchConnection	Gewährt die Berechtigung zum Erstellen einer neuen clusterübergreifenden Suchverbindung von einer Quell-Domain zu einer Ziel-Domain Diese Berechtigung ist veraltet. Verwenden Sie stattdessen CreateOutboundConnection	Schreiben	domain*		
CreatePackage	Gewährt die Berechtigung zum Hinzufügen eines Pakets zur Verwendung mit OpenSearch-Service-Domains	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateServiceRole	Gewährt die Berechtigung zum Erstellen der serviceverknüpften Rolle, die für Amazon OpenSearch Service-Domains erfoderlich ist, die VPC-Zugriff nutzen	Schreiben			
CreateVpcEndpoint	Gewährt die Berechtigung zum Erstellen eines von Amazon OpenSearch Service verwalteten VPC-Schnittstellenendpunkts	Schreiben			
DeleteDataSource	Gewährt die Berechtigung zum Löschen der Datenquelle für die OpenSearch-Service-Domain	Schreiben	domain*		
DeleteDomain	Gewährt die Berechtigung zum Löschen einer Amazon OpenSearch Service-Domain und ihrer Daten	Schreiben	domain*		
DeleteElasticsearchDomain	Gewährt die Berechtigung zum Löschen einer OpenSearch Service-Domain und ihrer Daten Diese Berechtigung ist veraltet. Verwenden Sie stattdessen DeleteDomain	Schreiben	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteElasticsearchServiceRole	Gewährt die Berechtigung zum Löschen der serviceverknüpften Rolle, die für OpenSearch Service-Domains erfoderlich ist, die VPC-Zugriff nutzen. Diese Berechtigung ist veraltet. Sie können die IAM-API für das Löschen einer serviceverknüpften Rolle verwenden	Schreiben			
DeleteInboundConnection	Gewährt die Berechtigung für den Eigentümer der Ziel-Domain, eine vorhandene eingehende clusterübergreifende Suchverbindung zu löschen	Schreiben			
DeleteInboundCrossClusterSearchConnection	Gewährt die Berechtigung für den Eigentümer der Ziel-Domain, eine vorhandene eingehende clusterübergreifende Suchverbindung zu löschen Diese Berechtigung ist veraltet. Verwenden Sie stattdessen DeleteInboundConnection	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteOutboundConnection	Gewährt die Berechtigung für den Eigentümer der Quell-Domain, eine vorhandene ausgehende clusterübergreifende Suchverbindung zu löschen	Schreiben			
DeleteOutboundCrossClusterSearchConnection	Gewährt die Berechtigung für den Eigentümer der Quell-Domain, eine vorhandene ausgehende clusterübergreifende Suchverbindung zu löschen Diese Berechtigung ist veraltet. Verwenden Sie stattdessen DeleteOutboundConnection	Schreiben			
DeletePackage	Gewährt die Berechtigung zum Löschen eines Pakets aus dem OpenSearch Service. Das Paket darf keiner Domain zugeordnet sein	Schreiben			
DeleteVpcEndpoint	Gewährt die Berechtigung zum Löschen eines von Amazon OpenSearch Service verwalteten Schnittstellen-VPC-Endpunkts	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDomain	Gewährt die Berechtigung zum Anzeigen einer Beschreibung der Domain-Konfiguration für die angegebene OpenSearch Service-Domain, einschließlich Domain-ID, Service-Endpunkt und ARN	Lesen	domain*		
DescribeDomainAutoTunes	Gewährt die Berechtigung zum Anzeigen der Auto-Tune-Konfiguration der Domain für die angegebene OpenSearch Service-Domain einschließlich AutoTune-Status und Wartungspläne	Lesen	domain*		
DescribeDomainChangeProgress	Gewährt die Berechtigung zum Anzeigen des Fortschritts der Detailstufe einer OpenSearch-Service-Domain	Lesen	domain*		
DescribeDomainConfig	Gewährt die Berechtigung zum Anzeigen einer Beschreibung der Konfigurationsoptionen und des Status einer OpenSearch Service-Domain	Lesen	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDomainHealth	Gewährt die Berechtigung zum Anzeigen von Informationen über den Zustand von Domains und Knoten, die Standby-Availability-Zone, die Anzahl der Knoten pro Availability Zone und die Anzahl der Shards pro Knoten	Lesen	domain*		
DescribeDomainNodes	Gewährt die Berechtigung zum Anzeigen von Informationen über die für die Domain konfigurierten Knoten und deren Konfigurationen – Knoten-ID, Knotentyp, Knotenstatus, Availability Zone, Instance-Typ und Speicher	Lesen	domain*		
DescribeDomains	Gewährt die Berechtigung zum Anzeigen einer Beschreibung der Domain-Konfiguration für bis zu fünf angegebene OpenSearch Service-Domains	Auflisten	domain*		
DescribeDryRunProgress	Gewährt die Berechtigung zum Beschreiben des Status einer vor einer Aktualisierung durchgeführten Validierungsprüfung an einer OpenSearch-Service-Domain	Lesen	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeElasticsearchDomain	Gewährt die Berechtigung zum Anzeigen einer Beschreibung der Domain-Konfiguration für die angegebene OpenSearch Service-Domain, einschließlich Domain-ID, Service-Endpunkt und ARN Diese Berechtigung ist veraltet. Verwenden Sie stattdessen DescribeDomain	Lesen	domain*		
DescribeElasticsearchDomainConfig	Gewährt die Berechtigung zum Anzeigen einer Beschreibung der Konfiguration und des Status einer OpenSearch Service-Domain Diese Berechtigung ist veraltet. Verwenden Sie stattdessen DescribeDomainConfig	Lesen	domain*		
DescribeElasticsearchDomains	Gewährt die Berechtigung zum Anzeigen einer Beschreibung der Domain-Konfiguration für bis zu fünf angegebene Amazon OpenSearch-Domains Diese Berechtigung ist veraltet. Verwenden Sie stattdessen DescribeDomains	Auflisten	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeElasticsearchInstanceTypeLimits	Gewährt die Berechtigung zum Anzeigen von Instance-Anzahl, Speicher und Hauptknoten-Limits für die gegebene OpenSearch-Version und den gegebenen Instance-Typ. Diese Berechtigung ist veraltet. Verwenden Sie stattdessen DescribeInstanceTypeLimits	Auflisten			
DescribeInboundConnections	Gewährt die Berechtigung zum Auflisten aller eingehenden clusterübergreifenden Suchverbindungen für eine Ziel-Domain	Auflisten			
DescribeInboundCrossClusterSearchConnections	Gewährt die Berechtigung zum Auflisten aller eingehenden clusterübergreifenden Suchverbindungen für eine Ziel-Domain Diese Berechtigung ist veraltet. Verwenden Sie stattdessen DescribeInBoundConnections	Auflisten			
DescribeInstanceTypeLimits	Gewährt die Berechtigung zum Anzeigen von Instance-Anzahl, Speicher und Hauptknoten-Limits für die gegebene Engine-Version und den gegebenen Instance-Typ	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeOutboundConnections	Gewährt die Berechtigung zum Auflisten aller ausgehenden clusterübergreifenden Suchverbindungen für eine Quell-Domain	Auflisten			
DescribeOutboundCrossClusterSearchConnections	Gewährt die Berechtigung zum Auflisten aller ausgehenden clusterübergreifenden Suchverbindungen für eine Quell-Domain Diese Berechtigung ist veraltet. Verwenden Sie stattdessen DescribeOutboundConnections	Auflisten			
DescribePackages	Gewährt die Berechtigung zum Beschreiben aller Pakete, die für OpenSearch Service-Domains verfügbar sind	Lesen			
DescribeReservedElasticsearchInstanceOfferings	Gewährt die Berechtigung zum Abrufen von Reserved Instance-Angeboten für Amazon OpenSearch Service. Diese Berechtigung ist veraltet. Verwenden Sie stattdessen DescribeReservedInstanceOfferings	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeReservedElasticsearchInstances	Gewährt die Berechtigung zum Abrufen von OpenSearch Services Reserved Instances, die bereits erworben wurden. Diese Berechtigung ist veraltet. Verwenden Sie stattdessen DescribeReservedInstances	Auflisten			
DescribeReservedInstanceOfferings	Gewährt die Berechtigung zum Abrufen Reserved Instance-Angebote für OpenSearch Service	Auflisten			
DescribeReservedInstances	Gewährt die Berechtigung zum Abrufen von OpenSearch Services Reserved Instances, die bereits erworben wurden	Auflisten			
DescribeVpcEndpoints	Gewährt die Berechtigung zum Beschreiben von einem oder mehreren von Amazon OpenSearch Service verwalteten VPC-Schnittstellenendpunkten	Auflisten			
DissociatePackage	Gewährt die Berechtigung zum Aufheben der Zuordnung eines Pakets von der angegebenen OpenSearch Service-Domain	Schreiben	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ESCrossClusterGet	Gewährt die Berechtigung zum Senden von clusterübergreifenden Anforderungen an eine Ziel-Domain	Read	domain		
ESHttpDelete	Gewährt die Berechtigung zum Senden von HTTP DELETE-Anforderungen an die OpenSearch-APIs	Write	domain		
ESHttpGet	Gewährt die Berechtigung zum Senden von HTTP GET-Anforderungen an die OpenSearch-APIs	Read	domain		
ESHttpHead	Gewährt die Berechtigung zum Senden von HTTP HEAD-Anforderungen an die OpenSearch-APIs	Read	domain		
ESHttpPatch	Gewährt die Berechtigung zum Senden von HTTP PATCH-Anforderungen an die OpenSearch-APIs.	Write	domain		
ESHttpPost	Gewährt die Berechtigung zum Senden von HTTP POST-Anforderungen an die OpenSearch-APIs	Write	domain		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ESHttpPut	Gewährt die Berechtigung zum Senden von HTTP PUT-Anforderungen an die OpenSearch-APIs	Schreiben	domain		
GetCompatibleElasticsearchVersions	Gewährt die Berechtigung zum Abrufen der Liste der kompatiblen OpeanSearch- und Elastic-Versionen, auf die eine OpenSearch Service-Domain aktualisiert werden kann. Diese Berechtigung ist veraltet. Verwenden Sie stattdessen GetCompatibleVersions	Auflisten	domain*		
GetCompatibleVersions	Gewährt die Berechtigung zum Abrufen der Liste der kompatiblen Elastic-ersionen, auf die die OpenSearch Service-Domain aktualisiert werden kann	Auflisten	domain*		
GetDataSource	Gewährt die Berechtigung zum Abrufen der Datenquelle für die OpenSearch-Service-Domain	Lesen	domain*		
GetDomainMaintenanceStatus	Gewährt die Berechtigung zum Abrufen des Status der Wartungsaktion für den Knoten	Lesen	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetPackageVersionHistory	Gewährt die Berechtigung zum Abrufen des Versionsverlaufs für ein Paket	Lesen			
GetUpgradeHistory	Gewährt die Berechtigung zum Abrufen des Upgrade-Verlaufs für eine bestimmte OpenSearch Service-Domain	Lesen	domain*		
GetUpgradeStatus	Gewährt die Berechtigung zum Abrufen des Upgrade-Status für eine bestimmte OpenSearch Service-Domain	Lesen	domain*		
ListDataSources	Gewährt die Berechtigung zum Abrufen einer Liste von Datenquellen für die OpenSearch-Service-Domain	Auflisten	domain*		
ListDomainMaintenances	Gewährt die Berechtigung zum Abrufen einer Liste von Wartungsaktionen für die OpenSearch-Service-Domain	Auflisten	domain*		
ListDomainNames	Gewährt die Berechtigung zum Anzeigen der Namen aller OpenSearch Service-Domains, die dem aktuellen Benutzer gehören	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDomainsForPackage	Gewährt die Berechtigung zum Auflisten aller OpenSearch Service-Domains auf, denen ein Paket zugeordnet ist	Auflisten			
ListElasticsearchInstanceTypeDetails	Gewährt die Berechtigung zum Auflisten aller Instance-Typen und verfügbaren Funktionen für eine bestimmte OpenSearch-Version. Diese Berechtigung ist veraltet. Verwenden Sie stattdessen ListInstanceTypeDetails	Auflisten			
ListElasticsearchInstanceTypes	Gewährt die Berechtigung zum Auflisten aller EC2-Instance-Typen, die für eine gegebene OpenSearch-Version unterstützt werden	Auflisten			
ListElasticsearchVersions	Gewährt die Berechtigung zum Auflisten aller in Amazon OpenSearch Service unterstützten OpenSearch-Versionen. Diese Berechtigung ist veraltet. Verwenden Sie stattdessen ListVersions	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListInstanceTypeDetails	Gewährt die Berechtigung zum Auflisten aller Instance-Typen und verfügbaren Funktionen für eine bestimmte OpenSearch- oder Elasticsearch-Version	Auflisten			
ListPackagesForDomain	Gewährt die Berechtigung zum Auflisten aller Pakete, die einer OpenSearch-Service-Domain zugeordnet sind	Auflisten	domain*		
ListScheduledActions	Gewährt die Berechtigung zum Abrufen einer Liste von Konfigurationesänderungen, die für eine OpenSearch-Service-Domain geplant sind	Auflisten	domain*		
ListTags	Gewährt die Berechtigung zum Anzeigen aller Ressourcen-Tags einer OpenSearch-Service-Domain	Lesen	domain*		
ListVersions	Gewährt die Berechtigung zum Auflisten aller unterstützten OpenSearch- und Elasticsearch-Versionen in Amazon OpenSearch Service	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListVpcEndpointAccess	Gewährt die Berechtigung, Informationen über jeden AWS Principal abzurufen, der über einen Schnittstellen-VPC-Endpunkt auf eine bestimmte Domain von Amazon OpenSearch Service zugreifen darf.	Auflisten			
ListVpcEndpoints	Gewährt die Berechtigung zum Abrufen aller von Amazon OpenSearch Service verwalteten VPC-Endpunkte im aktuellen AWS-Konto und in der aktuellen Region	Auflisten			
ListVpcEndpointsForDomain	Gewährt die Berechtigung zum Abrufen aller von Amazon OpenSearch Service verwalteten VPC-Endpunkte, die einer bestimmten Domain zugeordnet sind	Auflisten			
PurchaseReservedElasticsearchInstanceOffering	Gewährt die Berechtigung zum Kauf von OpenSearch-Reserved-Instances. Diese Berechtigung ist veraltet. Verwenden Sie stattdessen PurchaseReservedInstanceOffering	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PurchaseReservedInstanceOffering	Gewährt die Berechtigung zum Kauf eines OpenSearch-Reserved-Instance-Angebots	Write			
RejectInboundConnection	Gewährt die Berechtigung für den Eigentümer der Ziel-Domain, eine eingehende clusterübergreifende Suchverbindungsanforderung abzulehnen	Schreiben			
RejectInboundCrossClusterSearchConnection	Gewährt die Berechtigung für den Eigentümer der Ziel-Domain, eine eingehende clusterübergreifende Suchverbindungsanforderung abzulehnen. Diese Berechtigung ist veraltet. Verwenden Sie stattdessen RejectInboundConnection	Schreiben			
RemoveTags	Gewährt die Berechtigung zum Entfernen von Ressourcen-Tags aus einer OpenSearch Service-Domain	Markierung	domain*		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RevokeVpcEndpointAccess	Gewährt die Berechtigung, den über einen Schnittstellen-VPC-Endpunkt bereitgestellten Zugriff auf eine Domain von Amazon OpenSearch Service zurückzuziehen	Schreiben			
StartDomainMaintenance	Gewährt die Berechtigung zum Einleiten der Wartung am Knoten	Schreiben	domain*		
StartElasticsearchServiceSoftwareUpdate	Gewährt die Berechtigung zum Starten des Service-Software-Updates einer Domain. Diese Berechtigung ist veraltet. Verwenden Sie stattdessen StartServiceSoftwareUpdate	Schreiben	domain*		
StartServiceSoftwareUpdate	Gewährt die Berechtigung zum Starten des Service-Software-Updates einer Domain	Schreiben	domain*		
UpdateDataSource	Gewährt die Berechtigung zum Aktualisieren der Datenquelle für die OpenSearch-Service-Domain	Schreiben	domain*		
UpdateDomainConfig	Gewährt die Berechtigung zum Ändern der Konfiguration einer OpenSearch-Domain, beispielsweise Instance-Typ oder Anzahl der Instances	Schreiben	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateElasticsearchDomainConfig	Gewährt die Berechtigung zum Ändern der Konfiguration einer OpenSearch-Domain, beispielsweise Instance-Typ oder Anzahl der Instances . Diese Berechtigung ist veraltet. Verwenden Sie stattdessen UpdateDomainConfig	Schreiben	domain*		
UpdatePackage	Gewährt die Berechtigung zum Aktualisieren eines Pakets zur Verwendung mit OpenSearch-Service-Domains	Schreiben			
UpdateScheduledAction	Gewährt die Berechtigung zum Verschieben einer geplanten Konfigurationsänderung an einer OpenSearch-Service-Domain auf einen späteren Zeitpunkt	Schreiben	domain*		
UpdateVpcEndpoint	Gewährt die Berechtigung zum Ändern eines von Amazon OpenSearch Service verwalteten Schnittstellen-VPC-Endpunkts	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpgradeDomain	Gewährt die Berechtigung zum Initiieren der Aktualisierung einer OpenSearch Service-Domain auf eine angegebene Version	Schreiben	domain*		
UpgradeElasticsearchDomain	Gewährt die Berechtigung zum Initiieren der Aktualisierung einer OpenSearch Service-Domain auf eine angegebene Version Diese Berechtigung ist veraltet. Verwenden Sie stattdessen UpgradeDomain	Schreiben	domain*		

Von Amazon OpenSearch Service definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
domain	`arn:${Partition}:es:${Region}:${Account}:domain/${DomainName}`	aws:ResourceTag/${TagKey}
es_role	`arn:${Partition}:iam::${Account}:role/aws-service-role/es.amazonaws.com/`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
	`AWSServiceRoleForAmazonOpenSearchService`	
opensearchservice_role	`arn:${Partition}:iam::${Account}:role/aws-service-role/opensearchservice.amazonaws.com/AWSServiceRoleForAmazonOpenSearchService`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon OpenSearch Service

Amazon OpenSearch Service definiert die folgenden Bedingungsschlüssel, die in einem `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüsseln, die in der Anforderung übergeben werden.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS OpsWorks

AWS OpsWorks (Servicepräfix: `opsworks`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS OpsWorks definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssignInstance	Gewährt die Berechtigung, eine registrierte Instance einer Ebene zuzuweisen	Schreiben	stack		
AssignVolume	Gewährt die Berechtigung, eins der registrierten Amazon-EBS-Volumes des Stacks einer angegebenen Instance zuzuweisen	Schreiben	stack		
AssociateElasticIp	Gewährt die Berechtigung, eine der registrierten elastischen IP-Adressen des Stacks	Schreiben	stack		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	einer angegebenen Instance zuzuweisen				
AttachElasticLoadBalancer	Gewährt die Berechtigung, einen Elastic Load Balancer an eine angegebene Ebene anzufügen	Schreiben	stack		
CloneStack	Gewährt die Berechtigung zum Erstellen eines Klons des angegebenen Clusters	Schreiben	stack		
CreateApp	Gewährt die Berechtigung zum Erstellen einer Anwendung für einen Cluster	Schreiben	stack		
CreateDeployment	Gewährt die Berechtigung zum Ausführen von Bereitstellungs- oder Stack-Befehlen	Schreiben	stack		
CreateInstance	Gewährt die Berechtigung zum Erstellen einer Instance in einem Stack	Schreiben	stack		
CreateLayer	Gewährt die Berechtigung zum Erstellen einer Ebene	Schreiben	stack		
CreateStack	Gewährt die Berechtigung zum Erstellen eines neuen Stacks	Schreiben			
CreateUserProfile	Gewährt die Berechtigung zum Erstellen eines neuen Benutzerprofils	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteApp	Gewährt die Berechtigung zum Löschen einer angegebenen Anwendung	Schreiben	stack		
DeleteInstance	Gewährt die Berechtigung zum Löscht einer angegebene Instance, wodurch die zugeordnete Amazon-EC2-Instance beendet wird	Schreiben	stack		
DeleteLayer	Gewährt die Berechtigung zum Löschen einer angegebenen Ebene	Schreiben	stack		
DeleteStack	Gewährt die Berechtigung zum Löschen eines angegebenen Stacks	Schreiben	stack		
DeleteUserProfile	Gewährt die Berechtigung zum Löschen eines Benutzerprofils	Schreiben			
DeregisterEcsCluster	Gewährt die Berechtigung zum Löschen eines Benutzerprofils	Schreiben	stack		
DeregisterElasticIp	Gewährt die Berechtigung zum Aufheben der Registrierung einer angegebenen elastischen IP-Adresse	Schreiben	stack		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeregisterInstance	Gewährt die Berechtigung zum Aufheben der Registrierung einer Amazon-EC2- oder On-Premises-Instance	Schreiben	stack		
DeregisterRdsDbInstance	Gewährt die Berechtigung zum Aufheben der Registrierung einer Amazon-RDS-Instance	Schreiben	stack		
DeregisterVolume	Gewährt die Berechtigung zum Aufheben der Registrierung eines Amazon-EBS-Volumes	Schreiben	stack		
DescribeAgentVersions	Gewährt die Berechtigung zum Beschreiben der verfügbaren AWS OpsWorks-Agentenversionen	Auflisten	stack		
DescribeApps	Gewährt die Berechtigung zum Anfordern einer Beschreibung für eine Gruppe von Anwendungen	Auflisten	stack		
DescribeCommands	Gewährt die Berechtigung zum Beschreiben der Ergebnisse bestimmter Befehle	Auflisten	stack		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDeployments	Gewährt die Berechtigung zum Anfordern einer Beschreibung für eine Gruppe von Bereitstellungen	Auflisten	stack		
DescribeEcsClusters	Gewährt die Berechtigung zum Beschreiben von Amazon-ECS-Clustern, die bei einem Stack registriert sind	Auflisten	stack		
DescribeElasticIps	Gewährt die Berechtigung zum Beschreiben elastischer IP-Adressen	Auflisten	stack		
DescribeElasticLoadBalancers	Gewährt die Berechtigung zum Beschreiben der Elastic-Load-Balancing-Instances eines Stacks	Auflisten	stack		
DescribeInstances	Gewährt die Berechtigung zum Anfordern einer Beschreibung für eine Gruppe von Instances	Auflisten	stack		
DescribeLayers	Gewährt die Berechtigung zum Anfordern einer Beschreibung für eine oder mehrere Ebenen in einem Stack	Auflisten	stack		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeLoadBasedAutoScaling	Gewährt die Berechtigung zum Beschreiben von lastbasierten Konfigurationen des Auto Scaling für bestimmte Ebenen	Auflisten	stack		
DescribeMyUserProfile	Gewährt die Berechtigung zum Beschreiben der SSH-Informationen eines Benutzers	Auflisten			
DescribeOperatingSystems	Gewährt die Berechtigung zum Beschreiben der Betriebssysteme, die von AWS OpsWorks Stacks unterstützt werden	Auflisten			
DescribePermissions	Gewährt die Berechtigung zum Beschreiben der Berechtigungen für einen Stack	Auflisten	stack		
DescribeRaidArrays	Gewährt die Berechtigung zum Beschreiben der RAID-Arrays einer Instance	Auflisten	stack		
DescribeRdsDbInstances	Gewährt die Berechtigung zum Beschreiben von Amazon-RDS-Instances	Auflisten	stack		
DescribeServiceErrors	Gewährt die Berechtigung zum Beschreiben von AWS-OpsWorks-Servicefehlern	Auflisten	stack		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeStackProvisioningParameters	Gewährt die Berechtigung zum Beschreiben der Bereitstellungsparameter eines Stacks	Auflisten	stack		
DescribeStackSummary	Gewährt die Berechtigung zum Beschreiben der Anzahl von Ebenen und Anwendungen in einem Stack sowie der Anzahl von Instances in jedem Status (z. B. running_setup oder online)	Auflisten	stack		
DescribeStacks	Gewährt die Berechtigung zum Anfordern einer Beschreibung für eine oder mehrere Stacks	Auflisten	stack		
DescribeTimeBasedAutoScaling	Gewährt die Berechtigung zum Beschreiben der zeitbasierten Konfigurationen für das Auto Scaling für angegebene Instances	Auflisten	stack		
DescribeUserProfiles	Gewährt die Berechtigung zum Beschreiben der angegebenen Benutzer	Auflisten			
DescribeVolumes	Gewährt die Berechtigung zum Beschreiben der Amazon-EBS-Volumes einer Instance	Auflisten	stack		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DetachElasticLoadBalancer	Gewährt die Berechtigung zum Trennen einer Elastic-Load-Balancing-Instance von ihrer Ebene	Schreiben	stack		
DisassociateElasticIp	Gewährt die Berechtigung zum Trennen einer elastischen IP-Adresse von ihrer Instance	Schreiben	stack		
GetHostnameSuggestion	Gewährt die Berechtigung zum Abrufen eines generierten Hostnamens für die angegebene Ebene, der auf dem aktuellen Hostnamen design basiert	Lesen	stack		
GrantAccess	Gewährt die Berechtigung, einer Windows-Instance für einen bestimmten Zeitraum RDP-Zugriff zu erteilen	Schreiben	stack		
ListTags	Gewährt die Berechtigung, eine Liste der Tags zurückzugeben, die dem angegebenen Stack oder der angegebenen Ebene zugewiesen sind	Auflisten	stack		
RebootInstance	Gewährt die Berechtigung, eine angegebene Instance neu zu starten	Schreiben	stack		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RegisterEcsCluster	Gewährt die Berechtigung zum Registrieren eines angegebenen Amazon-ECS-Clusters bei einem Stack	Schreiben	stack		
RegisterElasticIp	Gewährt die Berechtigung zum Registrieren einer elastischen IP-Adresse beim angegebenen Stack	Schreiben	stack		
RegisterInstance	Gewährt die Berechtigung zum Registrieren von Instances, die außerhalb von AWS OpsWorks erstellt wurden, bei einem angegebenen Stack	Schreiben	stack		
RegisterRdsDbInstance	Gewährt die Berechtigung zum Registrieren einer Amazon-RDS-Instance bei einem Stack	Schreiben	stack		
RegisterVolume	Gewährt die Berechtigung zum Registrieren eines Amazon-EBS-Volumes bei einem angegebenen Stack	Schreiben	stack		
SetLoadBasedAutoScaling	Gewährt die Berechtigung zur Angabe der lastbasierten Konfiguration für das Auto Scaling für eine angegebene Ebene	Schreiben	stack		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SetPermission	Gewährt die Berechtigung zur Angabe der Berechtigungen eines Benutzers	Berechtigungsverwaltung	stack		
SetTimeBasedAutoScaling	Gewährt die Berechtigung zur Angabe der zeitbasierten Konfiguration für das Auto Scaling für die angegebene Instance	Schreiben	stack		
StartInstance	Gewährt die Berechtigung zum Starten einer angegebenen Instance	Schreiben	stack		
StartStack	Gewährt die Berechtigung zum Starten der Instances eines Stacks	Schreiben	stack		
StopInstance	Gewährt die Berechtigung zum Anhalten einer angegebenen Instance	Schreiben	stack		
StopStack	Gewährt die Berechtigung zum Anhalten eines angegebenen Stacks	Schreiben	stack		
TagResource	Gewährt die Berechtigung, Tags auf einen Stack oder eine Ebene anzuwenden	Markierung	stack		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UnassignInstance	Gewährt die Berechtigung zum Aufheben der Zuordnung einer registrierten Instance zu all ihren Ebenen	Schreiben	stack		
UnassignVolume	Gewährt die Berechtigung zum Aufheben der Zuordnung eines Amazon-EBS-Volumes	Schreiben	stack		
UntagResource	Gewährt die Berechtigung, Tags aus einem Stack oder einer Ebene zu entfernen	Markierung	stack		
UpdateApp	Gewährt die Berechtigung zum Aktualisieren einer bestimmten Anwendung	Schreiben	stack		
UpdateElasticIp	Gewährt die Berechtigung zum Aktualisieren des Namens einer registrierten elastischen IP-Adresse	Schreiben	stack		
UpdateInstance	Gewährt die Berechtigung zum Aktualisieren einer bestimmten Instance	Schreiben	stack		
UpdateLayer	Gewährt die Berechtigung zum Aktualisieren einer bestimmten Ebene	Schreiben	stack		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateMyUserProfile	Gewährt die Berechtigung zum Aktualisieren des öffentlichen SSH-Schlüssels eines Benutzers	Schreiben			
UpdateRdsDbInstance	Gewährt die Berechtigung zum Aktualisieren einer Amazon-RDS-Instance	Schreiben	stack		
UpdateStack	Gewährt die Berechtigung zum Aktualisieren eines bestimmten Stacks	Schreiben	stack		
UpdateUserProfile	Gewährt die Berechtigung zum Aktualisieren eines bestimmten Benutzerprofils	Berechtigungsverwaltung			
UpdateVolume	Gewährt die Berechtigung zum Aktualisieren des Namens oder Mounting-Punkts eines Amazon-EBS-Volumes	Schreiben	stack		

Von AWS OpsWorks definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
stack	`arn:${Partition}:opsworks:${Region}:${Account}:stack/${StackId}/`	

Bedingungsschlüssel für AWS OpsWorks

OpsWorks besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS OpsWorks Configuration Management

AWS OpsWorks Configuration Management (Servicepräfix: `opsworks-cm`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS OpsWorks Configuration Management definierte Aktionen
- Von AWS OpsWorks Configuration Management definierte Ressourcentypen
- Bedingungsschlüssel für AWS OpsWorks Configuration Management

Von AWS OpsWorks Configuration Management definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen.

Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateNode	Gewährt die Berechtigung zum Zuordnen eines Knoten zu einem Konfigurationsmanagement-Server	Write			
CreateBackup	Gewährt die Berechtigung zum Erstellen eines Backups für den angegebenen Server	Write			
CreateServer	Gewährt die Berechtigung zum Erstellen eines neuen Servers	Write			
DeleteBackup	Gewährt die Berechtigung zum Löschen des angegebenen Backups und möglicher weise dessen S3-Buckets	Write			
DeleteServer	Gewährt die Berechtigung zum Löschen des angegebenen Servers mit seinem entsprechenden CloudFormation-Stack und möglicher weise dem S3 Bucket	Write			
DescribeAccountAttributes	Gewährt die Berechtigung zum Beschreiben der Servicelimits für das Benutzerkonto	List			
DescribeBackups	Gewährt die Berechtigung zum Beschreiben eines einzelnen Backups, aller Backups eines angegebenen	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Servers oder aller Backups des Benutzerkontos				
DescribeEvents	Gewährt die Berechtigung zum Beschreiben aller Ereignisse des angegebenen Servers	List			
DescribeNodeAssociationStatus	Gewährt die Berechtigung zum Beschreiben des Mappingsstatus des angegebenen Knoten-Tokens und des angegebenen Servers	List			
DescribeServers	Gewährt die Berechtigung zum Beschreiben des angegebenen Servers oder aller Server des Benutzerkontos	List			
DisassociateNode	Gewährt die Berechtigung zum Aufheben der Mapping eines angegebenen Knotens von einem Server	Write			
ExportServerEngineAttribute	Gewährt die Berechtigung zum Exportieren eines Engine-Attributs von einem Server	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags, die auf den angegebenen Server oder das Backup angewendet werden	Read			
RestoreServer	Gewährt die Berechtigung zum Anwenden eines Backups auf den angegebenen Server. Tauscht möglicherweise die EC2-Instance aus (falls angegeben)	Write			
StartMaintenance	Gewährt die Berechtigung zum sofortigen Start der Serverwartung	Write			
TagResource	Gewährt die Berechtigung zum Anwenden von Tags auf den angegebenen Server oder das Backup	Markieren			
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags von dem angegebenen Server oder des Backups	Markieren			
UpdateServer	Gewährt die Berechtigung zum Aktualisieren allgemeiner Servereinstellungen	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateServerEngineAttributes	Gewährt die Berechtigung zum Aktualisieren der für die Konfigurationsverwaltung spezifischen Servereinstellungen	Write			

Von AWS OpsWorks Configuration Management definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
server	`arn:${Partition}:opsworks-cm::${Account}:server/${ServerName}/${UniqueId}`	
backup	`arn:${Partition}:opsworks-cm::${Account}:backup/${ServerName}-{Date-and-Time-Stamp-of-Backup}`	

Bedingungsschlüssel für AWS OpsWorks Configuration Management

OpsworksCM besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Organizations

AWS Organizations (Dienstpräfix:`organizations`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Organizations definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptHandshake	Gewährt die Berechtigung zum Senden einer Antwort an den Sender eines Handshakes, mit dem der in der Handshake-Anforderung vorgeschlagenen Aktion zugestimmt wird	Schreiben	handshake*		iam:CreateServiceLinkedRole
AttachPolicy	Gewährt die Berechtigung zum Anfügen einer Richtlinie an einen Root, eine Organisationseinheit oder ein individuelles Konto	Schreiben	policy*		
			account		
			organizationalunit		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			root		
				organizations:PolicyType	
CancelHandshake	Gewährt die Berechtigung zum Abbrechen eines Handshakes	Schreiben	handshake*		
CloseAccount	Erteilt die Erlaubnis AWS-Konto , eine zu schließen, die jetzt Teil einer Organizations ist, entweder innerhalb der Organisation erstellt wurde oder zu deren Beitritt eingeladen wurde	Schreiben	account*		
CreateAccount	Erteilt die Berechtigung AWS-Konto , eine Person zu erstellen, die automatisch Mitglied der Organisation wird, und zwar mit den Anmeldeinformationen, mit denen die Anfrage gestellt wurde	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGovCloudAccount	Erteilt die Erlaubnis, ein AWS GovCloud (US-) Konto zu erstellen	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateOrganization	Gewährt die Berechtigung zum Erstellen einer Organisation. Das Konto mit den Anmeldeinformationen, das den CreateOrganization Vorgang aufruft, wird automatisch zum Verwaltungskonto der neuen Organisation	Schreiben			iam:CreateServiceLinkedRole
CreateOrganizationalUnit	Gewährt die Berechtigung zum Erstellen einer Organisationseinheit (OU) innerhalb einer Root- oder übergeordneten OU	Schreiben	organizationalunit		
			root		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePolicy	Erteilt die Berechtigung zum Erstellen einer Richtlinie, die Sie einem Stamm, einer Organisationseinheit (OU) oder einer Einzelperson zuordnen können AWS-Konto	Schreiben		organizations:PolicyType aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeclineHandshake	Gewährt die Berechtigung zum Ablehnen einer Handshake-Anforderung. Dadurch wird der Status des Handshakes auf DECLINED gesetzt und die Anforderung wird praktisch deaktiviert	Schreiben	handshake*		
DeleteOrganization	Gewährt die Berechtigung zum Löschen der Organisation	Schreiben			
DeleteOrganizationalUnit	Gewährt die Berechtigung zum Löschen einer Organisationseinheit (OU) aus einer Root- oder einer anderen OU	Schreiben	organizationalunit*		
DeletePolicy	Gewährt die Berechtigung zum Löschen einer Richtlinie aus der Organisation	Schreiben	policy*		
				organizations:PolicyType	
DeleteResourcePolicy	Gewährt die Berechtigung zum Löschen einer Ressourcenrichtlinie aus der Organisation	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeregisterDelegatedAdministrator	Erteilt die Berechtigung, das angegebene Mitglied AWS-Konto als delegierten Administrator für den AWS Dienst abzumelden, der durch angegeben ist ServicePrincipal	Schreiben	account*		
				organizations:ServicePrincipal	
DescribeAccount	Gewährt die Berechtigung zum Abrufen organisationsbezogener Details zum angegebenen Konto	Lesen	account*		
DescribeCreateAccountStatus	Gewährt die Berechtigung zum Abrufen des aktuellen Status einer asynchronen Anforderung zum Erstellen eines Kontos	Lesen			
DescribeEffectivePolicy	Gewährt die Berechtigung zum Abrufen der effektiven Richtlinie für ein Konto	Lesen	account*		
				organizations:PolicyType	
DescribeHandshake	Gewährt die Berechtigung zum Abrufen von Details zu einem zuvor angeforderten Handshake	Lesen	handshake*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeOrganization	Gewährt die Berechtigung zum Abrufen von Details zu der Organisation, zu der die aufrufenden Anmeldeinformationen gehören	Lesen			
DescribeOrganizationalUnit	Gewährt die Berechtigung zum Abrufen von Details zu einer Organisationseinheit (OU)	Lesen	organizationalunit*		
DescribePolicy	Gewährt die Berechtigung zum Abrufen von Details zu einer Richtlinie	Lesen	policy*		
				organizations:PolicyType	
DescribeResourcePolicy	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Ressourcenrichtlinie	Lesen			
DetachPolicy	Gewährt die Berechtigung zum Trennen einer Richtlinie von einem Ziel-Root, einer organisatorischen Einheit oder einem Konto	Schreiben	policy*		
			account		
			organizationalunit		
			root		
				organizations:PolicyType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisableAWSServiceAccess	Erteilt die Berechtigung, die Integration eines AWS Dienstes (des Dienstes, der von angegeben ist ServicePrincipal) mit AWS Organizations zu deaktivieren	Schreiben		organizations:ServicePrincipal	
DisablePolicyType	Gewährt die Berechtigung zum Deaktivieren eines Organisationsrichtlinientyps in einem Root	Schreiben	root*		
				organizations:PolicyType	
EnableAWSServiceAccess	Erteilt die Erlaubnis, die Integration eines AWS Dienstes (des Dienstes, der von spezifiziert ist ServicePrincipal) mit AWS Organizations zu ermöglichen	Schreiben		organizations:ServicePrincipal	
EnableAllFeatures	Gewährt die Berechtigung zum Starten des Prozesses, der alle Funktionen in einer Organisation aktiviert und die Organisation von der Unterstützung nur der „Konsolidierte Fakturierung“-Funktionen hochstuft	Schreiben			
EnablePolicyType	Gewährt die Berechtigung zum Aktivieren eines Richtlinientyps in einem Root	Schreiben	root*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				organizations:PolicyType	
InviteAccountToOrganization	Erteilt die Erlaubnis, eine Einladung an eine andere Person zu senden und sie zu bitten AWS-Konto, Ihrer Organisation als Mitglieds konto beizutreten	Schreiben	account		
				aws:RequestTag/${TagKey} aws:TagKeys	
LeaveOrganization	Gewährt die Berechtigung zum Entfernen eines Mitglieds kontos aus seiner übergeord neten Organisation	Schreiben			
ListAWSServiceAccessForOrganization	Erteilt die Berechtigung zum Abrufen der Liste der AWS Dienste, für die Sie die Integration mit Ihrer Organisation aktiviert haben	Auflisten			
ListAccounts	Gewährt die Berechtigung zum Auflisten aller Konten in der Organisation	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAccountsForParent	Gewährt die Berechtigung zum Auflisten der Konten in einer Organisation, die in einem Root oder einer Organisationseinheit (OU) enthalten sind	Auflisten	organizationalunit		
			root		
ListChildren	Gewährt die Berechtigung zum Auflisten aller OUs oder Konten, die in einer übergeordneten OU oder im Root enthalten sind	Auflisten	organizationalunit		
			root		
ListCreateAccountStatus	Gewährt die Berechtigung zum Auflisten asynchroner Kontoerstellungsanforderungen, die derzeit für die Organisation verfolgt werden	Auflisten			
ListDelegatedAdministrators	Erteilt die Berechtigung, die AWS Konten aufzulisten, die in dieser Organisation als delegierte Administratoren bezeichnet wurden	Auflisten		organizations:ServicePrincipal	
ListDelegatedServicesForAccount	Erteilt die Berechtigung, die AWS Dienste aufzulisten, für die das angegebene Konto ein delegierter Administrator in dieser Organisation ist	Auflisten	account*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListHandshakesForAccount	Gewährt die Berechtigung zum Auflisten aller Handshakes, die einem Konto zugeordnet sind	Auflisten			
ListHandshakesForOrganization	Gewährt die Berechtigung zum Auflisten der Handshakes, die der Organisation zugeordnet sind	Auflisten			
ListOrganizationalUnitsForParent	Gewährt die Berechtigung zum Auflisten aller Organisationseinheiten (OUs) in einer übergeordneten Organisationseinheit oder im Root	Auflisten	organizationalunit		
			root		
ListParents	Gewährt die Berechtigung zum Auflisten des Roots oder der Organisationseinheiten (OUs), der/die einer untergeordneten OU oder einem Konto unmittelbar übergeordnet ist/sind	Auflisten	account		
			organizationalunit		
ListPolicies	Gewährt die Berechtigung zum Auflisten aller Richtlinien in einer Organisation	Auflisten		organizations:PolicyType	
ListPoliciesForTarget	Gewährt die Berechtigung zum Auflisten aller Richtlinien, die direkt an einen Root, eine Organisationseinheit (OU) oder ein Konto angefügt sind	Auflisten	account		
			organizationalunit		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			root		
				organizations:PolicyType	
ListRoots	Gewährt die Berechtigung zum Auflisten aller Roots, die in der Organisation definiert sind	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten aller Tags für die angegebene Ressource	Auflisten	account		
			organizationalunit		
			policy		
			resourcepolicy		
			root		
ListTargetsForPolicy	Gewährt die Berechtigung zum Auflisten aller Roots, OUs und Konten, an die eine Richtlinie angefügt ist	Auflisten	policy*		
				organizations:PolicyType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
MoveAccount	Gewährt die Berechtigung zum Verschieben eines Kontos aus dem aktuellen Root oder der aktuellen OU in einen anderen übergeordneten Root oder eine andere übergeordnete OU	Schreiben	account*		
			organizationalunit*		
			root*		
PutResourcePolicy	Gewährt die Berechtigung zum Erstellen oder Aktualisieren einer Ressourcenrichtlinie	Schreiben	resourcepolicy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RegisterDelegatedAdministrator	Erteilt die Erlaubnis, das angegebene Mitgliedskonto zu registrieren, um die Organisationsfunktionen des AWS Dienstes zu verwalten, der angegeben ist von ServicePrincipal	Schreiben	account*		
				organizations:ServicePrincipal	
RemoveAccountFromOrganization	Gewährt die Berechtigung zum Entfernen des angegebenen Kontos aus der Organisation	Schreiben	account*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Tags zur angegebenen Ressource	Markieren	account		
			organizationalunit		
			policy		
			resourcepolicy		
			root		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen eines oder mehrerer Tags aus der angegebenen Ressource	Tagging	account		
			organizationalunit		
			policy		
			resourcepolicy		
			root		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateOrganizationalUnit	Gewährt die Berechtigung zum Umbenennen einer Organisationseinheit (OU)	Schreiben	organizationalunit*		
UpdatePolicy	Gewährt die Berechtigung zum Aktualisieren einer Richtlinie mit neuem Namen, neuer Beschreibung oder neuem Inhalt	Schreiben	policy*		
				organizations:PolicyType	

Von AWS Organizations definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
account	`arn:${Partition}:organizations::${Account}:account/o-${OrganizationId}/${AccountId}`	aws:ResourceTag/${TagKey}
handshake	`arn:${Partition}:organizations::${Account}:handshake/o-${OrganizationId}/${HandshakeType}/h-${HandshakeId}`	

Ressourcentypen	ARN	Bedingungsschlüssel
organization	`arn:${Partition}:organizations::${Account}:organization/o-${OrganizationId}`	
organizationalunit	`arn:${Partition}:organizations::${Account}:ou/o-${OrganizationId}/ou-${OrganizationalUnitId}`	aws:ResourceTag/${TagKey}
policy	`arn:${Partition}:organizations::${Account}:policy/o-${OrganizationId}/${PolicyType}/p-${PolicyId}`	aws:ResourceTag/${TagKey}
resourcepolicy	`arn:${Partition}:organizations::${Account}:resourcepolicy/o-${OrganizationId}/rp-${ResourcePolicyId}`	aws:ResourceTag/${TagKey}
awspolicy	`arn:${Partition}:organizations::aws:policy/${PolicyType}/p-${PolicyId}`	
root	`arn:${Partition}:organizations::${Account}:root/o-${OrganizationId}/r-${RootId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Organizations

AWS Organizations definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString
organizations:PolicyType	Filtert den Zugriff nach den angegebenen Richtlinientypnamen	String
organizations:ServicePrincipal	Filtert den Zugriff nach den angegebenen Servicepr inzipalnamen	String

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Outposts

AWS Outposts (Dienstpräfix:`outposts`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Outposts definierte Aktionen
- Von AWS Outposts definierte Ressourcentypen
- Bedingungsschlüssel für AWS Outposts

Von AWS Outposts definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelCapacityTask	Erteilt die Berechtigung, eine Capacity-Aufgabe abzubrechen	Schreiben	outpost*		
CancelOrder	Gewährt die Berechtigung zum Abbrechen eines Auftrags	Schreiben			
CreateOrder	Gewährt die Berechtigung zum Erstellen eines Auftrags	Schreiben	outpost*		
CreateOutpost	Gewährt die Berechtigung zum Erstellen eines Outpost	Schreiben	site*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePrivateConnectivityConfig	Gewährt die Berechtigung zum Erstellen einer privaten Konnektivitätskonfiguration	Schreiben			
CreateSite	Gewährt die Berechtigung zum Erstellen einer Site	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteOutpost	Gewährt die Berechtigung zum Löschen eines Outpost	Schreiben	outpost*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteSite	Gewährt die Berechtigung zum Löschen einer Website	Schreiben	site*		
GetCapacityTask	Erteilt die Berechtigung, Informationen über die angegebene Kapazität saufgabe abzurufen	Lesen	outpost*		
GetCatalogItem	Gewährt die Berechtigung zum Erhalten eines Katalogelements	Lesen			
GetConnection	Gewährt die Berechtigung zum Abrufen von Informationen die Verbindung für Ihren Outpost-Server zu erhalten	Lesen			
GetOrder	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Bestellung	Lesen			
GetOutpost	Gewährt die Berechtigung zum Abrufen von Informationen über den angegebenen Outpost	Lesen	outpost*		
GetOutpostInstanceTypes	Gewährt die Berechtigung zum Abrufen der Instance-Typen für den angegebenen Outpost	Lesen	outpost*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetOutpostSupportedInstanceTypes	Erteilt die Berechtigung, die unterstützten Instanztypen für den angegebenen Outpost abzurufen	Lesen	outpost*		
GetPrivateConnectivityConfig	Gewährt die Berechtigung zum Abrufen einer privaten Konnektivitätskonfiguration	Lesen			
GetSite	Gewährt die Berechtigung zum Abrufen einer Site	Lesen	site*		
GetSiteAddress	Gewährt die Berechtigung zum Abrufen einer Site-Adresse	Lesen	site*		
ListAssets	Gewährt die Berechtigung zum Auflisten der Komponenten für Ihr Outpost	Auflisten			
ListCapacityTasks	Erteilt die Erlaubnis, die Capacity-Aufgaben für Ihre aufzulisten AWS-Konto	Auflisten			
ListCatalogItems	Gewährt die Berechtigung zum Auflisten aller Katalogelemente	Auflisten			
ListOrders	Erteilt die Erlaubnis, die Bestellungen für Sie aufzulisten AWS-Konto	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListOutposts	Erteilt die Erlaubnis, die Outposts für dich aufzulisten AWS-Konto	Auflisten			
ListSites	Erteilt die Erlaubnis, die Websites für dich aufzulisten AWS-Konto	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen			
StartCapacityTask	Erteilt die Berechtigung zum Erstellen einer Capacity-Aufgabe	Schreiben	outpost*		
StartConnection	Gewährt die Berechtigung zum Starten einer Verbindung für Ihren Outpost-Server	Schreiben			
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren	outpost		
			site		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Tagging	outpost		
			site		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
UpdateOutpost	Gewährt die Berechtigung zum Aktualisieren eines Outposts	Schreiben	outpost*		
UpdateSite	Gewährt die Berechtigung, eine Website zu aktualisieren	Schreiben	site*		
UpdateSiteAddress	Gewährt die Berechtigung zum Aktualisieren der Standortadresse	Schreiben	site*		
UpdateSiteRackPhysicalProperties	Gewährt die Berechtigung zum Aktualisieren der physikalischen Eigenschaften eines Racks an einem Standort	Schreiben	site*		

Von AWS Outposts definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
outpost	`arn:${Partition}:outposts:${Region}:${Account}:outpost/${OutpostId}`	aws:ResourceTag/${TagKey}
site	`arn:${Partition}:outposts:${Region}:${Account}:site/${SiteId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Outposts

AWS Outposts definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Panorama

AWS Panorama (Servicepräfix: `panorama`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Panorama definierte Aktionen
- Von AWS Panorama definierte Ressourcentypen
- Bedingungsschlüssel für AWS Panorama

Von AWS Panorama definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateApplicationInstance	Gewährt die Berechtigung zum Erstellen einer AWS Panorama-Anwendungs-Instance	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	
CreateJobForDevices	Gewährt die Berechtigung zum Erstellen eines Auftrags für eine AWS-Panorama-Anwendung	Schreiben			
CreateNodeFromTemplateJob	Gewährt die Berechtigung zum Erstellen eines AWS-Panorama-Knotens	Schreiben			
CreatePackage	Gewährt die Berechtigung zum Erstellen eines AWS-Panorama-Pakets	Schreiben		aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey}	
CreatePackageImportJob	Gewährt die Berechtigung zum Erstellen eines AWS-Panorama-Pakets	Schreiben			
DeleteDevice	Gewährt die Berechtigung zum Aufheben der Registrierung einer AWS-Panorama-Appliance	Schreiben	device*		
DeletePackage	Gewährt die Berechtigung zum Löschen eines AWS-Panorama-Pakets	Schreiben	package*		
DeregisterPackageVersion	Gewährt die Berechtigung zum Aufheben der Registrierung einer AWS-Panorama-Paketversion	Schreiben	package*		
DescribeApplicationInstance	Gewährt die Berechtigung zum Anzeigen von Details zu einer AWS-Panorama-Anwendungs-Instance	Lesen	applicationInstance*		
DescribeApplicationInstanceDetails	Gewährt die Berechtigung zum Anzeigen von Details zu einer AWS-Panorama-Anwendungs-Instance	Lesen	applicationInstance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDevice	Gewährt die Berechtigung zum Anzeigen von Details zu einer AWS-Panorama-Appliance	Lesen	device*		
DescribeDeviceJob	Gewährt die Berechtigung zum Anzeigen von Details zu einer AWS-Panorama-Appliance	Lesen			
DescribeNode	Gewährt die Berechtigung zum Anzeigen von Details zu einem AWS-Panorama-Anwendungsknoten	Lesen			
DescribeNodeFromTemplateJob	Gewährt die Berechtigung zum Anzeigen von Details zu AWS-Panorama-Anwendungsknoten	Lesen			
DescribePackage	Gewährt die Berechtigung zum Anzeigen von Details zu einem AWS-Panorama-Paket	Lesen	package*		
DescribePackageImportJob	Gewährt die Berechtigung zum Anzeigen von Details zu einem AWS-Panorama-Paket	Lesen			
DescribePackageVersion	Gewährt die Berechtigung zum Anzeigen von Details zu einer AWS-Panorama-Paketversion	Lesen	package*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeSoftware [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen von Details zu einer Softwareversion für die AWS-Panorama-Appliance	Read			
GetWebSocketURL [nur Berechtigung]	Gewährt die Berechtigung zum Generieren eines WebSocket-Endpunkts für die Kommunikation mit AWS Panorama	Lesen			
ListApplicationInstanceDependencies	Gewährt die Berechtigung zum Abrufen einer Liste von Bereitstellungs-Instance-Abhängigkeiten in AWS-Panorama	Auflisten	applicationInstance*		
ListApplicationInstanceNodeInstances	Gewährt die Berechtigung zum Abrufen einer Liste von Knoten-Instancen von Anwendungs-Instancen in AWS-Panorama	Auflisten	applicationInstance*		
ListApplicationInstances	Gewährt die Berechtigung zum Abrufen einer Liste von Anwendungs-Instances in AWS-Panorama	Auflisten	device		
ListDevices	Gewährt die Berechtigung zum Abrufen einer Liste von Appliances in AWS Panorama	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDevicesJobs	Gewährt die Berechtigung zum Abrufen einer Liste von Aufträgen für eine AWS-Panorama-Appliance	Auflisten	device		
ListNodeFromTemplateJobs	Gewährt die Berechtigung zum Abrufen einer Liste der Knoten für eine AWS-Panorama-Appliance	Auflisten			
ListNodes	Gewährt die Berechtigung zum Abrufen einer Liste der Knoten in AWS-Panorama	Auflisten			
ListPackageImportJobs	Gewährt die Berechtigung zum Abrufen einer Liste der Pakete in AWS-Panorama	Auflisten			
ListPackages	Gewährt die Berechtigung zum Abrufen einer Liste der Pakete in AWS-Panorama	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Abrufen einer Liste von Tags für eine Ressource in AWS Panorama	Lesen	applicationInstance		
			device		
			package		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ProvisionDevice	Gewährt die Berechtigung zum Registrieren einer AWS-Panorama-Appliance	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	
RegisterPackageVersion	Gewährt die Berechtigung zur Registrierung einer AWS-Panorama-Paketversion	Schreiben	package*		
RemoveApplicationInstance	Gewährt die Berechtigung zum Entfernen einer AWS-Panorama-Anwendungs-Instance	Schreiben	applicationInstance*		
SignalApplicationInstanceNodeInstances	Erteilt die Erlaubnis, Kameraknoten in einer Anwendungs-Instance zu signalisieren, zu pausieren oder fortzufahren	Schreiben	applicationInstance*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Ressource in AWS Panorama	Markierung	applicationInstance		
			device		
			package		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Ressource in AWS Panorama	Markierung	applicationInstance		
			device		
			package		
				aws:TagKeys	
UpdateDeviceMetadata	Gewährt die Berechtigung zum Ändern der Grundeinstellungen für eine AWS-Panorama-Appliance	Write	device*		

Von AWS Panorama definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
device	`arn:${Partition}:panorama:${Region}:${Account}:device/${DeviceId}`	aws:ResourceTag/${TagKey}
package	`arn:${Partition}:panorama:${Region}:${Account}:package/${PackageId}`	aws:ResourceTag/${TagKey}
applicationInstance	`arn:${Partition}:panorama:${Region}:${Account}:applicationInstance/${ApplicationInstanceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Panorama

AWS Panorama definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für die zentrale AWS-Parnter-Kontoverwaltung

Die zentrale AWS-Partner-Kontoverwaltung (Service-Präfix: `partnercentral-account-management`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von der zentralen AWS-Partner-Kontoverwaltung definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociatePartnerAccount [nur Berechtigung]	Gewährt die Berechtigung zum Zuordnen eines Partnerkontos zu AWS-Konto	Schreiben			
AssociatePartnerUser	Gewährt die Berechtigung zum Zuordnen eines Partnerbenutzers zu einer IAM-Rolle	Schreiben			
DisassociatePartnerUser	Gewährt die Berechtigung zum Aufheben der Zuordnung	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	eines Partnerbenutzers zu einer IAM-Rolle				

Von der zentralen AWS-Partner-Kontoverwaltung definierte Ressourcentypen

Die zentrale AWS-Partner-Kontoverwaltung unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf die zentrale AWS-Partner-Kontoverwaltung zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für die zentrale Kontoverwaltung von AWS-Partner

Die zentrale Partner-Kontoverwaltung besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Payment Cryptography

AWS Payment Cryptography (Servicepräfix: `payment-cryptography`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Payment Cryptography definierte Aktionen

- Von AWS Payment Cryptography definierte Ressourcentypen
- Bedingungsschlüssel für AWS Payment Cryptography

Von AWS Payment Cryptography definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAlias	Gewährt die Berechtigung, einen benutzerfreundlichen Namen für einen Schlüssel zu erstellen	Schreiben	alias*		
			key*		
CreateKey	Gewährt die Berechtigung, einen eindeutigen, vom Kunden verwalteten Schlüssel für das AWS-Konto und die Region des Aufrufers zu erstellen	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	payment-cryptography:TagResource
DecryptData	Gewährt die Berechtigung, Geheimtextdaten mithilfe eines symmetrischen, asymmetrischen oder DUKPT-Datenverschlüsselungsschlüssels in Klartext zu entschlüsseln	Schreiben			
DeleteAlias	Gewährt die Berechtigung zum Löschen des angegebenen -Alias	Schreiben	alias*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteKey	Gewährt die Berechtigung, die Löschung eines Schlüssels zu planen	Schreiben	key*		
EncryptData	Gewährt die Berechtigung, Klartextdaten mithilfe eines symmetrischen, asymmetrischen oder DUKPT-Datenverschlüsselungsschlüssels in Geheimtext zu verschlüsseln	Schreiben			
ExportKey	Gewährt die Berechtigung, einen Schlüssel aus dem Service zu exportieren	Schreiben	key*		
GenerateCardValidationData	Gewährt die Berechtigung, kartenbezogene Daten mithilfe von Algorithmen wie Card Verification Values (CVV/CVV2), Dynamic Card Verification Values (DCVV/DCVv2) oder Card Security Codes (CSC) zu generieren, mit denen die Gültigkeit einer Magnetstreifenkarte überprüft wird	Schreiben			
GenerateMac	Gewährt die Berechtigung, ein MAC-Kryptogramm (Message Authentication Code) zu generieren	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GeneratePinData	Gewährt die Berechtigung, bei der Ausstellung neuer Karten oder der erneuten Kartenausstellung PIN-bezogene Daten wie PIN, PIN Verification Value (PVV), PIN-Block und PIN-Offset zu generieren	Schreiben			
GetAlias	Gewährt die Berechtigung, den mit einem aliasName verbundenen keyArn zurückzugeben	Lesen	alias*		
			key*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetKey	Gewährt die Berechtigung, detaillierte Informationen zum angegebenen Schlüssel zurückzugeben	Lesen	key*		
GetParametersForExport	Gewährt die Berechtigung, das Exporttoken und das Signaturschlüsselzertifikat abzurufen, um einen TR-34-Schlüsselexport zu initiieren	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetParametersForImport	Gewährt die Berechtigung, das Importtoken und das Wrapping-Schlüssel-Zertifikat abzurufen, um einen TR-34-Schlüsselimport zu initiieren	Lesen			
GetPublicKeyCertificate	Gewährt die Berechtigung, den öffentlichen Schlüssel aus einem Schlüssel der Klasse PUBLIC_KEY zurückzugeben	Lesen	key*		
ImportKey	Gewährt die Berechtigung, Schlüssel und Zertifikate für öffentliche Schlüssel zu importieren	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	payment-cryptography:TagResource
ListAliases	Gewährt die Berechtigung, eine Liste von Aliassen zurückzugeben, die für alle Schlüssel im AWS-Konto und in der Region des Aufrufers erstellt wurden	Auflisten			
ListKeys	Gewährt die Berechtigung, eine Liste von Schlüsseln zurückzugeben, die im AWS-Konto und in der Region des Aufrufers erstellt wurden	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung, eine Liste von Tags zurückzugeben, die im AWS-Konto und in der Region des Aufrufers erstellt wurden	Lesen	key		
ReEncryptData	Gewährt die Berechtigung, Geheimtext mithilfe symmetrischer, asymmetrischer oder DUKPT-Datenverschlüsselungsschlüssels neu zu verschlüsseln	Schreiben			
RestoreKey	Gewährt die Berechtigung, eine geplante Schlüssellöschung zu stornieren, wenn ein Schlüssel während der Wartezeit wiederhergestellt werden muss	Schreiben	key*		
StartKeyUsage	Gewährt die Berechtigung, einen deaktivierten Schlüssel zu aktivieren	Schreiben	key*		
StopKeyUsage	Gewährt die Berechtigung, einen aktivierten Schlüssel zu deaktivieren	Schreiben	key*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung, ein oder mehrere Tags für die angegebene Ressource hinzuzufügen oder zu überschreiben	Tagging	key*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TranslatePinData	Gewährt die Berechtigung, verschlüsselte PIN-Blöcke von und in die ISO-9564-Formate 0, 1, 3, 4 umzuwandeln	Schreiben			
UntagResource	Gewährt die Berechtigung, die angegebenen Tags aus der angegebenen Ressource zu entfernen	Tagging	key*		
				aws:TagKeys	
UpdateAlias	Gewährt die Berechtigung, den Schlüssel zu ändern, dem ein Alias zugewiesen ist, oder die Zuweisung zum aktuellen Schlüssel aufzuheben	Schreiben	alias*		
			key*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
VerifyAuthRequestCryptogram	Gewährt die Berechtigung, das Authorization Request Cryptogram (ARQC) für die Autorisierung einer EMV-Chip-Zahlungskarte zu verifizieren	Schreiben			
VerifyCardValidationData	Gewährt die Berechtigung, kartenbezogene Validierungsdaten mithilfe von Algorithmen wie Card Verification Values (CVV/CVV2), Dynamic Card Verification Values (DCVV/DCVv2) oder Card Security Codes (CSC) zu verifizieren	Schreiben			
VerifyMac	Gewährt die Berechtigung, den MAC (Message Authentication Code) von Eingabedaten anhand eines bereitgestellten MAC zu überprüfen	Schreiben			
VerifyPinData	Gewährt die Berechtigung, PIN-bezogene Daten wie PIN und PIN-Offset mithilfe von Algorithmen wie VISA PVV und IBM3624 zu verifizieren	Schreiben			

Von AWS Payment Cryptography definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der

Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
key	`arn:${Partition}:payment-cryptography:${Region}:${Account}:key/${KeyId}`	aws:ResourceTag/${TagKey} payment-cryptography:ResourceAliases
alias	`arn:${Partition}:payment-cryptography:${Region}:${Account}:alias/${Alias}`	payment-cryptography:ResourceAliases

Bedingungsschlüssel für AWS Payment Cryptography

AWS Payment Cryptography definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Schlüssel und dem Wert des Tags in der Anforderung für die angegebene Operation	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach Tags, die einem Schlüssel für die angegebene Operation zugewiesen sind	String

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert den Zugriff nach den Tag-Schlüsseln in der Anforderung für die angegeben Operation	ArrayOfString
payment-cryptography:CertificateAuthorityPublicKeyIdentifier	Filtert den Zugriff nach dem in der Anforderung CertificateAuthorityPublicKeyIdentifier angegebenen oder den ExportKey Operationen ImportKey, und	String
payment-cryptography:ImportKeyMaterial	Filtert den Zugriff nach dem Typ des Schlüsselmaterials RootCertificatePublicKey, das für den ImportKey Vorgang importiert wird [TrustedCertificatePublicKey,, Tr34KeyBlock, Tr31KeyBlock]	String
payment-cryptography:KeyAlgorithm	Filtert den Zugriff nach , die in der Anforderung für die CreateKey Operation KeyAlgorithm angegeben sind	String
payment-cryptography:KeyClass	Filtert den Zugriff nach , die in der Anforderung für die CreateKey Operation KeyClass angegeben sind	String
payment-cryptography:KeyUsage	Filtert den Zugriff nach , der in der Anforderung KeyClass angegeben oder einem Schlüssel für die CreateKey Operation zugeordnet ist	String
payment-cryptography:RequestAlias	Filtert den Zugriff nach Aliassen in der Anforderung für die angegebene Operation	String
payment-cryptography:ResourceAliases	Filtert den Zugriff nach Aliassen, die mit einem Schlüssel für die angegebene Operation verknüpft sind	ArrayOfString

Bedingungsschlüssel	Beschreibung	Typ
payment-cryptography:WrappingKeyIdentifier	Filtert den Zugriff nach dem in der Anforderung für die ExportKey Operationen ImportKey, und WrappingKeyIdentifier angegebenen .	String

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Payments

AWS Payments (Servicepräfix: `payments`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Payments definierte Aktionen
- Von AWS Payments definierte Ressourcentypen
- Bedingungsschlüssel für AWS Payments

Von AWS Payments definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt,

müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreatePaymentInstrument [nur Berechtigung]	Gewährt die Berechtigung, ein Zahlungsinstrument zu erstellen	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeletePaymentInstrument [nur Berechtigung]	Gewährt die Berechtigung, ein Zahlungsinstrument zu löschen	Schreiben			
GetPaymentInstrument [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Zahlungsinstrument	Auflisten			
GetPaymentStatus [nur Berechtigung]	Gewährt die Berechtigung, den Zahlungsstatus von Rechnungen abzurufen	Lesen			
ListPaymentPreferences [nur Berechtigung]	Gewährt die Berechtigung, Zahlungspräferenzen zu erhalten (bevorzugte Zahlungswährung, bevorzugte Zahlungsmethode usw.)	Auflisten			
MakePayment [nur Berechtigung]	Gewährt die Berechtigung, eine Zahlung zu tätigen, eine Zahlung zu authentifizieren, eine Zahlungsmethode zu überprüfen und ein Finanzantragsdokument für Advance Pay zu erstellen	Schreiben			
UpdatePaymentPreferences [nur Berechtigung]	Gewährt die Berechtigung, Zahlungspräferenzen zu aktualisieren (bevorzugte Zahlungswährung, bevorzugte Zahlungsmethode usw.)	Schreiben			

Von AWS Payments definierte Ressourcentypen

AWS Payments unterstützt nicht die Angabe eines Ressourcen-ARN im Element `Resource` einer IAM-Richtlinienanweisung. Um den Zugriff auf AWS Payments zuzulassen, geben Sie in Ihrer Richtlinie `"Resource": "*"` an.

Bedingungsschlüssel für AWS Payments

Payments besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Performance Insights

AWS Performance Insights (Servicepräfix: `pi`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Performance Insights definierte Aktionen
- Von AWS Performance Insights definierte Ressourcentypen
- Bedingungsschlüssel für AWS Performance Insights

Von AWS Performance Insights definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreatePerformanceAnalysisReport	Gewährt die Berechtigung zum Aufrufen der CreatePerformanceAnalysisReport-API, um einen Leistungsanalysebericht für eine angegebene DB-Instance zu erstellen	Schreiben	perf-reports-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeletePerformanceAnalysisReport	Gewährt die Berechtigung zum Aufrufen der DeletePerformanceAnalysisReport-API, um einen Leistungsanalysebericht für eine angegebene DB-Instance zu löschen	Schreiben	perf-reports-resource*		
DescribeDimensionKeys	Gewährt die Berechtigung zum Aufrufen der API DescribeDimensionKeys, um die Schlüssel der Top-N-Dimension für eine Metrik für einen bestimmten Zeitraum abzurufen	Lesen	metric-resource*		
GetDimensionKeyDetails	Gewährt die Berechtigung zum Aufrufen der API GetDimensionKeyDetails, um die Attribute der angegebenen Dimensionsgruppe abzurufen	Lesen	metric-resource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetPerformanceAnalysisReport	Gewährt die Berechtigung zum Aufrufen der GetPerformanceAnalysisReport-API, um einen Leistungsanalysebericht für eine angegebene DB-Instance abzurufen	Lesen	perf-reports-resource*		
GetResourceMetadata	Gewährt die Berechtigung zum Aufrufen der API GetResourceMetadata, um Metadaten für verschiedene Features abzurufen	Lesen	metric-resource*		
GetResourceMetrics	Gewährt die Berechtigung zum Aufrufen der API GetResourceMetrics-API, um PI-Metriken für eine Reihe von Datenquellen über einen Zeitraum abzurufen	Lesen	metric-resource*		
ListAvailableResourceDimensions	Gewährt die Berechtigung zum Aufrufen der API ListAvailableResourceDimensions, um Dimensionen abzurufen, die für jeden angegebenen Metriktyp auf einer bestimmten DB-Instance abgefragt werden können	Lesen	metric-resource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAvailableResourceMetrics	Gewährt die Berechtigung zum Aufrufen der API ListAvailableResourceMetrics, um Metriken abzurufen, die für jeden angegebenen Metriktyp auf einer bestimmten DB-Instance abgefragt werden können	Lesen	metric-resource*		
ListPerformanceAnalysisReports	Gewährt die Berechtigung zum Aufrufen der ListPerformanceAnalysisReports-API, um Leistungsanalyseberichte für eine angegebene DB-Instance aufzulisten	Auflisten	perf-reports-resource*		
ListTagsForResource	Gewährt die Berechtigung zum Aufrufen der ListTagsForResource-API, um Tags für eine Ressource aufzulisten	Auflisten	perf-reports-resource*		
TagResource	Gewährt die Berechtigung zum Aufrufen der TagResource-API zum Kennzeichnen einer Ressource	Markierung	perf-reports-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UntagResource	Gewährt die Berechtigung zum Aufrufen der UntagResource-API, um die Kennzeichnung einer Ressource aufzuheben	Markierung	perf-reports-resource*		
				aws:TagKeys	

Von AWS Performance Insights definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
metric-resource	`arn:${Partition}:pi:${Region}:${Account}:metrics/${ServiceType}/${Identifier}`	
perf-reports-resource	`arn:${Partition}:pi:${Region}:${Account}:perf-reports/${ServiceType}/${Identifier}/${ReportId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Performance Insights

AWS Performance Insights definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die

Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Personalize

Amazon Personalize (Servicepräfix: `personalize`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Personalize definierte Aktionen
- Von Amazon Personalize definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Personalize

Von Amazon Personalize definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateBatchInferenceJob	Gewährt die Berechtigung zum Erstellen einer Batch-Inferenz-Aufgabe	Schreiben	batchInferenceJob*		
CreateBatchSegmentJob	Gewährt die Berechtigung zum Erstellen eines Batch-Segment-Auftrags	Schreiben	batchSegmentJob*		
CreateCampaign	Gewährt die Berechtigung zum Erstellen einer Kampagne	Schreiben	campaign*		
CreateDataDeletionJob	Erteilt die Erlaubnis, einen Datenlöschauftrag zu erstellen	Schreiben	dataDeletionJob*		
CreateDataInsightsJob	Gewährt die Berechtigung zum Erstellen eines Auftrags für Datenerkenntnisse	Schreiben	dataInsightsJob*		
CreateDataset	Gewährt die Berechtigung zum Erstellen eines Dataset	Schreiben	dataset*		
CreateDatasetExportJob	Gewährt die Berechtigung zum Erstellen einer Dataset-Importaufgabe	Schreiben	datasetExportJob*		
CreateDatasetGroup	Gewährt die Berechtigung zum Erstellen einer Dataset-Gruppe	Write	datasetGroup*		
CreateDatasetImportJob	Gewährt die Berechtigung zum Erstellen einer Dataset-Importaufgabe	Write	datasetImportJob*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateEventTracker	Gewährt die Berechtigung zum Erstellen eines Ereignis-Trackers	Write	eventTracker*		
CreateFilter	Gewährt die Berechtigung zum Erstellen eines Filters	Schreiben	filter*		
CreateMetricAttribution	Gewährt die Berechtigung zum Erstellen eines VPC-Anhangs	Schreiben	metricAttribution*		
CreateRecommender	Gewährt die Berechtigung zum Erstellen eines Empfehlers	Schreiben	recommender*		
CreateSchema	Gewährt die Berechtigung zum Erstellen eines Schemas	Write	schema*		
CreateSolution	Gewährt die Berechtigung zum Erstellen einer Lösung	Write	solution*		
CreateSolutionVersion	Gewährt die Berechtigung zum Erstellen einer Lösungsversion	Write	solution*		
DeleteCampaign	Gewährt die Berechtigung zum Löschen einer Kampagne	Write	campaign*		
DeleteDataset	Gewährt die Berechtigung zum Löschen eines Dataset	Write	dataset*		
DeleteDatasetGroup	Gewährt die Berechtigung zum Löschen einer Dataset-Gruppe	Write	datasetGroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteEventTracker	Gewährt die Berechtigung zum Löschen eines Ereignis-Trackers	Write	eventTracker*		
DeleteFilter	Gewährt die Berechtigung zum Löschen eines Filters	Schreiben	filter*		
DeleteMetricAttribution	Gewährt die Berechtigung zum Löschen einer Erteilung	Schreiben	metricAttribution*		
DeleteRecommender	Gewährt die Berechtigung zum Löschen eines Empfehlers	Schreiben	recommender*		
DeleteSchema	Gewährt die Berechtigung zum Löschen eines Schemas	Write	schema*		
DeleteSolution	Gewährt die Berechtigung zum Löschen einer Lösung einschließlich aller Versionen der Lösung	Write	solution*		
DescribeAlgorithm	Gewährt die Berechtigung zum Beschreiben eines Algorithmus	Read	algorithm*		
DescribeBatchInferenceJob	Gewährt die Berechtigung zum Beschreiben einer Batch-Inferenz-Aufgabe	Lesen	batchInferenceJob*		
DescribeBatchSegmentJob	Gewährt die Berechtigung zum Beschreiben eines Batch-Segment-Auftrags	Lesen	batchSegmentJob*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeCampaign	Gewährt die Berechtigung zum Beschreiben einer Kampagne	Lesen	campaign*		
DescribeDataDeletionJob	Erteilt die Erlaubnis, einen Datenlöschauftrag zu beschreiben	Lesen	dataDeletionJob*		
DescribeDataInsightsJob	Gewährt die Berechtigung zum Beschreiben eines Auftrags für Datenerkenntnisse	Lesen	dataInsightsJob*		
DescribeDataset	Gewährt die Berechtigung zum Beschreiben eines Dataset	Lesen	dataset*		
DescribeDatasetExportJob	Gewährt die Berechtigung zum Beschreiben einer Dataset-Importaufgabe	Lesen	datasetExportJob*		
DescribeDatasetGroup	Gewährt die Berechtigung zum Beschreiben einer Dataset-Gruppe	Read	datasetGroup*		
DescribeDatasetImportJob	Gewährt die Berechtigung zum Beschreiben einer Dataset-Importaufgabe	Read	datasetImportJob*		
DescribeEventTracker	Gewährt die Berechtigung zum Beschreiben eines Ereignis-Trackers	Read	eventTracker*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeFeatureTransformation	Gewährt die Berechtigung zum Beschreiben einer Feature-Transformation	Read	featureTransformation*		
DescribeFilter	Gewährt die Berechtigung zum Beschreiben eines Filters	Lesen	filter*		
DescribeMetricAttribution	Gewährt die Berechtigung zum Beschreiben eines Attributs einer VPC	Lesen	metricAttribution*		
DescribeRecipe	Gewährt die Berechtigung zum Beschreiben eines Rezepts	Lesen	recipe*		
DescribeRecommender	Gewährt die Berechtigung zum Beschreiben eines Empfehlers	Lesen	recommender*		
DescribeSchema	Gewährt die Berechtigung zum Beschreiben eines Schemas	Read	schema*		
DescribeSolution	Gewährt die Berechtigung zum Beschreiben einer Lösung	Read	solution*		
DescribeSolutionVersion	Gewährt die Berechtigung zum Beschreiben einer Version einer Lösung	Lesen	solution*		
GetActionRecommendations	Gewährt die Berechtigung zum Abrufen einer Liste von empfohlenen Aktionen	Lesen	campaign*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDataInsights	Gewährt die Berechtigung zum Abrufen von Datenerkenntnissen aus einem Auftrag	Lesen	dataInsightsJob*		
GetPersonalizedRanking	Gewährt die Berechtigung, eine erneut geordnete Liste von Empfehlungen zu erhalten	Read	campaign*		
GetRecommendations	Gewährt die Berechtigung, eine Liste von Empfehlungen aus einer Kampagne zu erhalten	Read	campaign*		
GetSolutionMetrics	Gewährt die Berechtigung zum Abrufen von Metriken für eine Lösungsversion	Read	solution*		
ListBatchInferenceJobs	Gewährt die Berechtigung zum Auflisten einer Batch-Inferenz-Aufgabe	Auflisten			
ListBatchSegmentJobs	Gewährt die Berechtigung zum Auflisten von Batch-Segment-Aufträgen	Auflisten			
ListCampaigns	Gewährt die Berechtigung zum Auflisten von Kampagnen	Auflisten			
ListDataDeletionJobs	Erteilt die Erlaubnis, Datenlöschaufträge aufzulisten	Auflisten			
ListDataInsightsJobs	Gewährt die Berechtigung zum Auflisten von Aufträgen für Datenerkenntnisse	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDatasetExportJobs	Gewährt die Berechtigung zum Auflisten von Dataset-Importaufgaben	Auflisten			
ListDatasetGroups	Gewährt die Berechtigung zum Auflisten von Dataset-Gruppen	List			
ListDatasetImportJobs	Gewährt die Berechtigung zum Auflisten von Dataset-Importaufgaben	List			
ListDatasets	Gewährt die Berechtigung zum Auflisten von Datasets	List			
ListEventTrackers	Gewährt die Berechtigung zum Auflisten eines Ereignis-Trackers	List			
ListFilters	Gewährt die Berechtigung zum Auflisten von Filtern	Auflisten			
ListMetricAttributionMetrics	Gewährt die Berechtigung zum Auflisten von	Auflisten			
ListMetricAttributions	Gewährt die Berechtigung zum Auflisten von	Auflisten			
ListRecipes	Gewährt die Berechtigung zum Auflisten von Rezepten	Auflisten			
ListRecommenders	Gewährt die Berechtigung zum Auflisten von Empfehlern	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListSchemas	Gewährt die Berechtigung zum Auflisten von Schemas	List			
ListSolutionVersions	Gewährt die Berechtigung zum Auflisten von Versionen einer Lösung	List			
ListSolutions	Gewährt die Berechtigung zum Auflisten von Lösungen	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Auflisten			
PutActionInteractions	Gewährt die Berechtigung zum Eingeben von Aktionsinteraktionsdaten in Echtzeit	Schreiben			
PutActions	Gewährt die Berechtigung zum Erfassen von Aktionsdaten	Schreiben	dataset*		
PutEvents	Gewährt die Berechtigung zum Eingeben von Ereignisdaten in Echtzeit	Write			
PutItems	Gewährt die Berechtigung zum Erfassen von Artikeldaten	Write	dataset*		
PutUsers	Gewährt die Erlaubnis zum Erfassen von Benutzerdaten	Schreiben	dataset*		
StartRecommender	Gewährt die Berechtigung zum Starten eines Empfehlers.	Schreiben	recommender*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopRecommender	Gewährt die Berechtigung zum Stoppen eines Empfehlers.	Schreiben	recommender*		
StopSolutionVersionCreation	Gewährt die Berechtigung zum Erstellen einer Lösungsversion	Schreiben	solution*		
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren			
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Tagging			
UpdateCampaign	Gewährt die Berechtigung zum Aktualisieren einer Kampagne	Schreiben	campaign*		
UpdateDataset	Gewährt die Berechtigung zum Aktualisieren eines Dataset	Schreiben	dataset*		
UpdateMetricAttribution	Gewährt die Berechtigung zum Aktualisieren einer Flottenmetrik	Schreiben	metricAttribution*		
UpdateRecommender	Gewährt die Berechtigung zum Aktualisieren eines Empfehlers	Schreiben	recommender*		

Von Amazon Personalize definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
schema	`arn:${Partition}:personalize:${Region}:${Account}:schema/${ResourceId}`	
featureTransformation	`arn:${Partition}:personalize:${Region}:${Account}:feature-transformation/${ResourceId}`	
dataset	`arn:${Partition}:personalize:${Region}:${Account}:dataset/${ResourceId}`	
datasetGroup	`arn:${Partition}:personalize:${Region}:${Account}:dataset-group/${ResourceId}`	
datasetImportJob	`arn:${Partition}:personalize:${Region}:${Account}:dataset-import-job/${ResourceId}`	
dataInsightsJob	`arn:${Partition}:personalize:${Region}:${Account}:data-insights-job/${ResourceId}`	
datasetExportJob	`arn:${Partition}:personalize:${Region}:${Account}:dataset-export-job/${ResourceId}`	

Ressourcentypen	ARN	Bedingungsschlüssel
dataDeletionJob	arn:${Partition}:personalize:${Region}:${Account}:data-deletion-job/${ResourceId}	
solution	arn:${Partition}:personalize:${Region}:${Account}:solution/${ResourceId}	
campaign	arn:${Partition}:personalize:${Region}:${Account}:campaign/${ResourceId}	
eventTracker	arn:${Partition}:personalize:${Region}:${Account}:event-tracker/${ResourceId}	
recipe	arn:${Partition}:personalize:${Region}:${Account}:recipe/${ResourceId}	
algorithm	arn:${Partition}:personalize:${Region}:${Account}:algorithm/${ResourceId}	
batchInferenceJob	arn:${Partition}:personalize:${Region}:${Account}:batch-inference-job/${ResourceId}	
filter	arn:${Partition}:personalize:${Region}:${Account}:filter/${ResourceId}	
recommender	arn:${Partition}:personalize:${Region}:${Account}:recommender/${ResourceId}	
batchSegmentJob	arn:${Partition}:personalize:${Region}:${Account}:batch-segment-job/${ResourceId}	

Ressource ntypen	ARN	Bedingungsschlüssel
metricAttribution	`arn:${Partition}:personalize:${Region}:${Account}:metric-attribution/${ResourceId}`	

Bedingungsschlüssel für Amazon Personalize

Amazon Personalize besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Pinpoint

Amazon Pinpoint (Servicepräfix: `mobiletargeting`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Pinpoint definierte Aktionen
- Von Amazon Pinpoint definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Pinpoint

Von Amazon Pinpoint definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen.

Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateApp	Gewährt die Berechtigung zum Erstellen einer App	Schreiben	apps*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateCampaign	Gewährt die Berechtigung zum Erstellen einer Kampagne für eine App	Schreiben	app*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateEmailTemplate	Gewährt die Berechtigung zum Erstellen einer E-Mail-Vorlage	Schreiben	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
CreateExportJob	Gewährt die Berechtigung zum Erstellen eines Exportauftrags für das Exportieren von Endpunktdefinitionen in Amazon S3	Schreiben	app*		
CreateImportJob	Gewährt die Berechtigung zum Importieren von Endpunkt-Definitionen zum Erstellen eines Segments	Schreiben	app*		
CreateInAppTemplate	Gewährt die Berechtigung zum Erstellen einer Vorlage für In-App-Nachrichten	Schreiben	template*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateJourney	Gewährt die Berechtigung zum Erstellen eines Wegs für eine App	Schreiben	journeys*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreatePushTemplate	Gewährt die Berechtigung zum Erstellen einer Push-Benachrichtigungsvorlage	Schreiben	template*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateRecommenderConfiguration	Gewährt die Berechtigung zum Erstellen einer Amazon-Pinpoint-Konfiguration für ein Empfehler-Modell	Schreiben	recommenders*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSegment	Gewährt die Berechtigung zum Erstellen eines Segments basierend auf Endpunktdaten, die von Ihrer App an Pinpoint gemeldet wurden. Um einem Benutzer zu erlauben, ein Segment durch Importieren von Endpunkt-Daten, die nicht aus Pinpoint stammen, zu erstellen, erlauben Sie die Aktion mobiletargeting:CreateImportJob	Schreiben	app*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateSmsTemplate	Gewährt die Berechtigung zum Erstellen einer SMS-Nachrichten-Vorlage	Schreiben	template*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateVoiceTemplate	Gewährt die Berechtigung zum Erstellen einer Sprachnachrichten-Vorlage	Schreiben	template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeleteAdmChannel	Gewährt die Berechtigung zum Löschen des ADM-Kanals für eine App	Schreiben	channel*		
DeleteApnsChannel	Gewährt die Berechtigung zum Löschen des APNs-Kanals für eine App	Schreiben	channel*		
DeleteApnsSandboxChannel	Gewährt die Berechtigung zum Löschen des APNs-Sandbox-Kanals für eine App	Schreiben	channel*		
DeleteApnsVoipChannel	Gewährt die Berechtigung zum Löschen des APNs-VoIP-Kanals für eine App	Schreiben	channel*		
DeleteApnsVoipSandboxChannel	Gewährt die Berechtigung zum Löschen des APNs-VoIP-Sandbox-Kanals für eine App	Schreiben	channel*		
DeleteApp	Gewährt die Berechtigung zum Löschen einer bestimmten Kampagne	Schreiben	app*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteBaiduChannel	Gewährt die Berechtigung zum Löschen des Baidu-Kanals für eine App	Schreiben	channel*		
DeleteCampaign	Gewährt die Berechtigung zum Löschen einer bestimmten Kampagne	Schreiben	campaign*		
DeleteEmailChannel	Gewährt die Berechtigung zum Löschen des E-Mail-Kanals für eine App	Schreiben	channel*		
DeleteEmailTemplate	Gewährt die Berechtigung zum Löschen einer E-Mail-Vorlage oder einer E-Mail-Vorlagenversion	Schreiben	template*		
DeleteEndpoint	Gewährt die Berechtigung zum Löschen eines Endpunkts	Schreiben	endpoint*		
DeleteEventStream	Gewährt die Berechtigung zum Löschen des Ereignis-Stream für eine App	Schreiben	event-stream*		
DeleteGcmChannel	Gewährt die Berechtigung zum Löschen des GCM-Kanals für eine App	Schreiben	channel*		
DeleteInAppTemplate	Gewährt die Berechtigung zum Löschen einer Vorlage für In-App-Nachrichten oder einer Vorlagenversion für In-App-Nachrichten	Schreiben	template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteJourney	Gewährt die Berechtigung zum Löschen eines bestimmten Weges	Schreiben	journey*		
DeletePushTemplate	Gewährt die Berechtigung zum Löschen einer Push-Benachrichtigungs-Vorlage oder eine Version einer Push-Benachrichtigungs-Vorlage	Schreiben	template*		
DeleteRecommenderConfiguration	Gewährt die Berechtigung zum Löschen einer Amazon-Pinpoint-Konfiguration für ein Empfehler-Modell	Schreiben	recommender*		
DeleteSegment	Gewährt die Berechtigung zum Löschen eines bestimmten Segments	Schreiben	segment*		
DeleteSmsChannel	Gewährt die Berechtigung zum Löschen des SMS-Kanals für eine App	Schreiben	channel*		
DeleteSmsTemplate	Gewährt die Berechtigung zum Löschen einer SMS-Nachrichtenvorlage oder einer SMS-Nachrichtenvorlagen-Version	Schreiben	template*		
DeleteUserEndpoints	Gewährt die Berechtigung zum Löschen aller Endpunkte, die einer Benutzer-ID zugeordnet sind	Schreiben	user*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteVoiceChannel	Gewährt die Berechtigung zum Löschen des Voice-Kanals für eine App	Schreiben	channel*		
DeleteVoiceTemplate	Gewährt die Berechtigung zum Löschen einer Sprachnachrichten-Vorlage oder eine Sprachnachrichten-Vorlagen-Version	Schreiben	template*		
GetAdmChannel	Gewährt die Berechtigung zum Abrufen von Informationen über den Amazon Device Messaging (ADM)-Kanal für eine App	Lesen	channel*		
GetApnsChannel	Gewährt die Berechtigung zum Abrufen von Informationen zum APNs-Kanal für eine App	Lesen	channel*		
GetApnsSandboxChannel	Gewährt die Berechtigung zum Abrufen von Informationen zum APNs-Sandbox-Kanal für eine App	Lesen	channel*		
GetApnsVoipChannel	Gewährt die Berechtigung zum Abrufen von Informationen zum APNs-VoIP-Kanal für eine App	Lesen	channel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetApnsVoipSandboxChannel	Gewährt die Berechtigung zum Abrufen von Informationen zum APNs-VoIP-Sandbox-Kanal für eine App	Lesen	channel*		
GetApp	Gewährt die Berechtigung zum Abrufen von Informationen zu einer bestimmten App in Ihrem Amazon-Pinpoint-Konto	Lesen	app*		
GetApplicationDateRangeKpi	Gewährt die Berechtigung zum Abrufen (der Abfragen) von voraggregierten Daten für eine Standardmetrik, die für eine Anwendung gilt	Lesen	application-metrics*		
GetApplicationSettings	Gewährt die Berechtigung zum Abrufen der Standardeinstellungen für eine App	Auflisten	app*		
GetApps	Gewährt die Berechtigung zum Abrufen einer Liste von Apps in Ihrem Amazon-Pinpoint-Konto	Lesen	apps*		
GetBaiduChannel	Gewährt die Berechtigung zum Abrufen von Informationen zum Baidu-Kanal für eine App	Lesen	channel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetCampaign	Gewährt die Berechtigung zum Abrufen von Informationen zu einer bestimmten Kampagne	Lesen	campaign*		
GetCampaignActivities	Gewährt die Berechtigung zum Abrufen von Informationen zu den Aktivitäten, die von einer Kampagne durchgeführt werden	Auflisten	campaign*		
GetCampaignDateRangeKpi	Gewährt die Berechtigung zum Abrufen (der Abfragen) von voraggregierten Daten für eine Standardmetrik, die für eine Kampagne gilt	Lesen	campaign-metrics*		
GetCampaignVersion	Gewährt die Berechtigung zum Abrufen von Informationen zu einer bestimmten Kampagnen-Version	Lesen	campaign*		
GetCampaignVersions	Gewährt die Berechtigung zum Abrufen von Informationen zu den aktuellen und vorherigen Versionen einer Kampagne	Auflisten	campaign*		
GetCampaigns	Gewährt die Berechtigung zum Abrufen von Informationen zu allen Kampagnen für eine App	Auflisten	app*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetChannels	Gewährt die Berechtigung zum Abrufen aller Kanalinformationen für Ihre App	Auflisten	channels*		
GetEmailChannel	Gewährt die Berechtigung zum Abrufen von Informationen über den E-Mail-Kanal in einer App	Lesen	channel*		
GetEmailTemplate	Gewährt die Berechtigung zum Abrufen von Informationen über eine bestimmte oder die aktive Version einer E-Mail-Vorlage	Lesen	template*		
GetEndpoint	Gewährt die Berechtigung zum Abrufen von Informationen zu einem bestimmten Endpunkt	Lesen	endpoint*		
GetEventStream	Gewährt die Berechtigung zum Abrufen von Informationen zum Ereignis-Stream für eine App	Lesen	event-stream*		
GetExportJob	Gewährt die Berechtigung zum Abrufen von Informationen zu einem bestimmten Exportauftrag	Lesen	export-job*		
GetExportJobs	Gewährt die Berechtigung zum Abrufen einer Liste aller Exportaufträge für eine App	Auflisten	app*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetGcmChannel	Gewährt die Berechtigung zum Abrufen von Informationen zum GCM-Kanal für eine App	Lesen	channel*		
GetImportJob	Gewährt die Berechtigung zum Abrufen von Informationen zu einem bestimmten Importauftrag	Lesen	import-job*		
GetImportJobs	Gewährt die Berechtigung zum Abrufen von Informationen zu allen Importaufträgen für eine App	Auflisten	app*		
GetInAppMessages	Gewährt die Berechtigung zum Abrufen von In-App-Nachrichten für die angegebene Endpunkt-ID	Lesen	app*		
GetInAppTemplate	Gewährt die Berechtigung zum Abrufen von Informationen über eine bestimmte oder die aktive Version einer In-App-Nachrichten-Vorlage	Lesen	template*		
GetJourney	Gewährt die Berechtigung zum Abrufen von Informationen zu einem bestimmten Weg	Lesen	journey*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetJourneyDateRangeKpi	Gewährt die Berechtigung zum Abrufen (der Abfragen) von voraggregierten Daten für eine Standard-Einbindungsmetrik, die für einen Weg gilt	Lesen	journey-metrics*		
GetJourneyExecutionActivityMetrics	Gewährt die Berechtigung zum Abrufen (der Abfragen) von voraggregierten Daten für eine Standard-Ausführungsmetrik, die für eine Weg-Aktivität gilt	Lesen	journey-execution-activity-metrics*		
GetJourneyExecutionMetrics	Gewährt die Berechtigung zum Abrufen (der Abfragen) von voraggregierten Daten für eine Standard-Ausführungsmetrik, die für einen Weg gilt	Lesen	journey-execution-metrics*		
GetJourneyRunExecutionActivityMetrics	Gewährt die Berechtigung zum Abrufen (der Abfragen) von voraggregierten Daten für eine Standard-Ausführungsmetrik, die für eine Weg-Aktivität gilt	Lesen	journey*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetJourneyRunExecutionMetrics	Gewährt die Berechtigung zum Abrufen (der Abfragen) von voraggregierten Daten für eine Standard-Ausführungsmetrik, die für einen Weg gilt	Lesen	journey*		
GetJourneyRuns	Gewährt die Berechtigung zum Abrufen von Informationen zu allen Wegen für eine App	Auflisten	journey*		
GetPushTemplate	Gewährt die Berechtigung zum Abrufen von Informationen über eine bestimmte oder die aktive Version einer Push-Benachrichtigungs-Vorlage	Lesen	template*		
GetRecommenderConfiguration	Gewährt die Berechtigung zum Abrufen von Informationen über eine Amazon-Pinpoint-Konfiguration für ein Empfehler-Modell	Lesen	recommender*		
GetRecommenderConfigurations	Gewährt die Berechtigung zum Abrufen von Informationen zu allen Konfigurationen des Empfehlungsmodells, die einem Amazon-Pinpoint-Konto zugeordnet sind	Auflisten	recommenders*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetReports [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von MobileTargeting:GetReports	Lesen	reports*		
GetSegment	Gewährt die Berechtigung zum Abrufen von Informationen zu einem bestimmten Segment	Lesen	segment*		
GetSegmentExportJobs	Gewährt die Berechtigung zum Abrufen von Informationen zu Aufträgen, die Endpunkt-Definitionen von Segmenten nach Amazon S3 exportieren	Auflisten	segment*		
GetSegmentImportJobs	Gewährt die Berechtigung zum Abrufen von Informationen zu Aufträgen, die Segmente durch Importieren von Endpunkt-Definitionen erstellen	Auflisten	segment*		
GetSegmentVersion	Gewährt die Berechtigung zum Abrufen von Informationen zu einer bestimmten Segmentversion	Lesen	segment*		
GetSegmentVersions	Gewährt die Berechtigung zum Abrufen von Informationen zu den aktuellen und vorherigen Versionen eines Segments	Auflisten	segment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetSegments	Gewährt die Berechtigung zum Abrufen von Informationen zu den Segmenten für eine App	Auflisten	app*		
GetSmsChannel	Gewährt die Berechtigung zum Abrufen von Informationen über den SMS-Kanal in einer App	Lesen	channel*		
GetSmsTemplate	Gewährt die Berechtigung zum Abrufen von Informationen über eine bestimmte oder die aktive Version einer SMS-Nachrichten-Vorlage	Lesen	template*		
GetUserEndpoints	Gewährt die Berechtigung zum Abrufen von Informationen über die Endpunkte, die einer Benutzer-ID zugeordnet sind	Lesen	user*		
GetVoiceChannel	Gewährt die Berechtigung zum Abrufen von Informationen über den Voice-Kanal in einer App	Lesen	channel*		
GetVoiceTemplate	Gewährt die Berechtigung zum Abrufen von Informationen über eine bestimmte oder die aktive Version einer Sprachnachrichten-Vorlage	Lesen	template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListJourneys	Gewährt die Berechtigung zum Abrufen von Informationen zu allen Wegen für eine App	Auflisten	app*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen	app		
			campaign		
			journey		
			segment		
			template		
ListTemplateVersions	Gewährt die Berechtigung zum Abrufen aller Versionen einer bestimmten Vorlage	Auflisten	template*		
ListTemplates	Gewährt die Berechtigung zum Abrufen von Metadaten zu den abgefragten Vorlagen	Auflisten	templates*		
PhoneNumberValidate	Gewährt die Berechtigung zum Abrufen von Metadaten für eine Telefonnummer, z. B. Nummerntyp (mobil, Festnetz oder VoIP), Standort und Anbieter	Lesen	phone-number-validate*		
PutEventStream	Gewährt die Berechtigung zum Erstellen oder Aktualisieren eines Ereignis-Streams für eine App	Schreiben	event-stream*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutEvents	Gewährt die Berechtigung zum Erstellen oder Aktualisieren von Ereignissen für eine App	Schreiben	events*		
RemoveAttributes	Gewährt die Berechtigung zum Entfernen der Attribute für eine App	Schreiben	attribute*		
SendMessages	Gewährt die Berechtigung zum Senden einer SMS-Nachricht oder Push-Benachrichtigung an bestimmte Endpunkte	Schreiben	messages*		
SendOTPMessage	Gewährt die Berechtigung, einen OTP-Code an einen Benutzer Ihrer Anwendung zu senden	Schreiben	otp*		
SendUsersMessages	Gewährt die Berechtigung zum Senden einer SMS-Nachricht oder Push-Benachrichtigung an alle Endpunkte, die einer bestimmten Benutzer-ID zugeordnet sind	Schreiben	messages*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Ressource	Markieren	app		
			campaign		
			journey		
			segment		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			template		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Ressource	Markierung	app		
			campaign		
			journey		
			segment		
			template		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateAdmChannel	Gewährt die Berechtigung zum Aktualisieren des Amazon Device Messaging (ADM)-Kanals für eine App	Schreiben	channel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateApnsChannel	Gewährt die Berechtigung zum Löschen des Apple Push Notification Service (APNs)-Kanals für eine App	Schreiben	channel*		
UpdateApnsSandboxChannel	Gewährt die Berechtigung zum Aktualisieren des Apple Push Notification Service (APNs)-Sandbox-Kanals für eine App	Schreiben	channel*		
UpdateApnsVoipChannel	Gewährt die Berechtigung zum Löschen des Apple Push Notification Service (APNs)-VoIP-Kanals für eine App	Schreiben	channel*		
UpdateApnsVoipSandboxChannel	Gewährt die Berechtigung zum Aktualisieren des Apple Push Notification Service (APNs)-VoIP-Sandbox-Kanals für eine App	Schreiben	channel*		
UpdateApplicationSettings	Gewährt die Berechtigung zum Aktualisieren der Standardeinstellungen für eine App	Schreiben	app*		
UpdateBaiduChannel	Gewährt die Berechtigung zum Aktualisieren des Baidu-Kanals für eine App	Schreiben	channel*		
UpdateCampaign		Schreiben	campaign*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Gewährt die Berechtigung zum Aktualisieren einer bestimmten Kampagne			aws:RequestTag/${TagKey} aws:TagKeys	
UpdateEmailChannel	Gewährt die Berechtigung zum Aktualisieren des E-Mail-Kanals für eine App	Schreiben	channel*		
UpdateEmailTemplate	Gewährt die Berechtigung zum Aktualisieren einer bestimmten E-Mail-Vorlage unter derselben Version zum Generieren einer neuen Version	Schreiben	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateEndpoint	Gewährt die Berechtigung zum Erstellen eines Endpunkts oder zum Aktualisieren der Informationen für einen Endpunkt	Schreiben	endpoint*		
UpdateEndpointsBatch	Gewährt die Berechtigung zum Erstellen oder Aktualisieren von Endpunkten als Batchvorgang	Schreiben	app*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateGcmChannel	Gewährt die Berechtigung zum Aktualisieren des Firebase Cloud Messaging (FCM)- oder Google Cloud Messaging (GCM)-API-Schlüssels, der das Senden von Push-Benachrichtigungen an Ihre Android-App erlaubt	Schreiben	channel*		
UpdateInAppTemplate	Gewährt die Berechtigung zum Aktualisieren einer bestimmten In-App-Nachrichten-Vorlage unter derselben Version oder zum Generieren einer neuen Version	Schreiben	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateJourney	Gewährt die Berechtigung zum Aktualisieren eines bestimmten Weges	Schreiben	journey*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateJourneyState	Gewährt die Berechtigung zum Aktualisieren eines bestimmten Weg-Status	Schreiben	journey*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdatePushTemplate	Gewährt die Berechtigung zum Aktualisieren einer bestimmten Push-Benachrichtigungs-Vorlage unter derselben Version oder zum Generieren einer neuen Version	Schreiben	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateRecommenderConfiguration	Gewährt die Berechtigung zum Aktualisieren einer Amazon-Pinpoint-Konfiguration für ein Empfehler-Modell	Schreiben	recommender*		
UpdateSegment	Gewährt die Berechtigung zum Aktualisieren eines bestimmten Segments	Schreiben	segment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateSmsChannel	Gewährt die Berechtigung zum Aktualisieren des SMS-Kanals für eine App	Schreiben	channel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateSmsTemplate	Gewährt die Berechtigung zum Aktualisieren einer bestimmten SMS-Vorlage unter derselben Version zum Generieren einer neuen Version	Schreiben	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTemplateActiveVersion	Gewährt die Berechtigung zum Aktualisieren des aktiven Versionsparameters einer bestimmten Vorlage	Schreiben	template*		
UpdateVoiceChannel	Gewährt die Berechtigung zum Aktualisieren des Voice-Kanals für eine App	Schreiben	channel*		
UpdateVoiceTemplate	Gewährt die Berechtigung zum Aktualisieren einer bestimmten Sprachnachrichten-Vorlage unter derselben Version zum Generieren einer neuen Version	Schreiben	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
VerifyOTPMessage	Gewährt die Berechtigung, die Gültigkeit von Einmalpasswörtern (OTPs) zu überprüfen	Schreiben	verify-otp*		

Von Amazon Pinpoint definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
app	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}`	aws:ResourceTag/${TagKey}
apps	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/*`	
campaign	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/campaigns/${CampaignId}`	aws:ResourceTag/${TagKey}
journey	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys/${JourneyId}`	aws:ResourceTag/${TagKey}
journeys	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys`	
segment	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/segments/${SegmentId}`	aws:ResourceTag/${TagKey}
template	`arn:${Partition}:mobiletargeting:${Region}:${Account}:templates/${TemplateName}/${TemplateType}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
templates	arn:${Partition}:mobiletargeting:${Region}:${Account}:templates	
recommender	arn:${Partition}:mobiletargeting:${Region}:${Account}:recommenders/${RecommenderId}	
recommenders	arn:${Partition}:mobiletargeting:${Region}:${Account}:recommenders/*	
phone-number-validate	arn:${Partition}:mobiletargeting:${Region}:${Account}:phone/number/validate	
channels	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/channels	
channel	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/channels/${ChannelType}	
event-stream	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/eventstream	
events	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/events	
messages	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/messages	

Ressourcentypen	ARN	Bedingungsschlüssel
verify-otp	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/verify-otp	
otp	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/otp	
attribute	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/attributes/${AttributeType}	
user	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/users/${UserId}	
endpoint	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/endpoints/${EndpointId}	
import-job	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/jobs/import/${JobId}	
export-job	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/jobs/export/${JobId}	
application-metrics	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/kpis/daterange/${KpiName}	
campaign-metrics	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/campaigns/${CampaignId}/kpis/daterange/${KpiName}	

Ressourcentypen	ARN	Bedingungsschlüssel
journey-metrics	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys/${JourneyId}/kpis/daterange/${KpiName}`	
journey-execution-metrics	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys/${JourneyId}/execution-metrics`	
journey-execution-activity-metrics	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys/${JourneyId}/activities/${JourneyActivityId}/execution-metrics`	
reports	`arn:${Partition}:mobiletargeting:${Region}:${Account}:reports`	

Bedingungsschlüssel für Amazon Pinpoint

Amazon Pinpoint definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach einem Schlüssel, der in der Anforderung vorhanden ist, die der Benutzer an den Pinpoint-Service sendet	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert den Zugriff anhand eines Tag-Schlüssel-Wert-Paares	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach der Liste aller Tag-Schlüsselnamen, die in der Anforderung vorhanden sind, die der Benutzer an den Pinpoint-Service sendet	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Pinpoint Email Service

Amazon Pinpoint Email Service (Servicepräfix: `ses`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Pinpoint Email Service definierte Aktionen
- Von Amazon Pinpoint Email Service definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Pinpoint Email Service

Von Amazon Pinpoint Email Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den

Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateConfigurationSet	Gewährt die Berechtigung zum Erstellen eines Konfigurationssatzes	Write		ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateConfigurationSetEventDestination	Gewährt die Berechtigung zum Erstellen eines Konfigurationssatz-Ereignisziels	Write	configuration-set* ses:ApiVersion aws:ResourceTag/${TagKey}		
CreateDedicatedIpPool	Gewährt die Berechtigung zum Erstellen eines neuen Pools dedizierter IP-Adressen	Write		ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateDeliverabilityTestReport	Gewährt die Berechtigung zum Erstellen eines neuen prädiktiven Posteingangs-Platzierungstests	Write	identity* ses:ApiVersion		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEmailIdentity	Gewährt die Berechtigung, den Prozess der Überprüfung einer E-Mail-Identität zu starten	Write		ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
DeleteConfigurationSet	Gewährt die Berechtigung zum Löschen eines vorhandenen Konfigurationssatzes	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteConfigurationSetEventDestination	Gewährt die Berechtigung zum Löschen eines Ereignisziels	Write	configuration-set*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteDedicatedIpPool	Gewährt die Berechtigung zum Löschen eines dedizierten IP-Pools	Write	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteEmailIdentity	Gewährt die Berechtigung zum Löschen einer zuvor verifizierten E-Mail-Identität	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetAccount	Gewährt die Berechtigung, Informationen über den Status und die Funktionen des E-Mail-Versands zu erhalten	Read		ses:ApiVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBlacklistReports	Gewährt die Berechtigung zum Abrufen einer Liste der Ablehnungslisten, auf denen Ihre dedizierten IP-Adressen angezeigt werden	Read		ses:ApiVersion	
GetConfigurationSet	Gewährt die Berechtigung zum Abrufen von Informationen über einen vorhandenen Konfigurationssatz	Read	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetConfigurationSetEventDestinations	Gewährt die Berechtigung zum Abrufen einer Liste von Ereigniszielen, die mit einem Konfigurationssatz verknüpft sind	Read	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDedicatedIp	Gewährt die Berechtigung, Informationen über eine dedizierte IP-Adresse zu erhalten	Read		ses:ApiVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDedicatedIps	Gewährt die Berechtigung zum Auflisten der dedizierten IP-Adressen, die mit Ihrem Konto verknüpft sind	Read	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDeliverabilityDashboardOptions	Gewährt die Berechtigung zum Abrufen des Status des Zustellbarkeits-Dashboards	Read		ses:ApiVersion	
GetDeliverabilityTestReport	Gewährt die Berechtigung zum Abrufen der Ergebnisse eines prädiktiven Tests zur Platzierung im Posteingang	Read	deliverability-test-report*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDomainDeliverabilityCampaign	Gewährt die Erlaubnis zum Abrufen aller Zustellbarkeitsdaten für eine bestimmte Kampagne	Read		ses:ApiVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDomainStatisticsReport	Gewährt die Berechtigung zum Abrufen der Posteingangsplatzierungs- und Interaktionsraten für die Domain, die Sie zum Senden von E-Mails verwenden	Read	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetEmailIdentity	Gewährt die Berechtigung, Informationen über eine bestimmte Identität zu erhalten, die mit Ihrem Konto verknüpft ist	Read	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListConfigurationSets	Gewährt die Berechtigung, alle mit Ihrem Konto verknüpften Konfigurationssätze aufzulisten	List		ses:ApiVersion	
ListDedicatedIpPools	Gewährt die Berechtigung, alle dedizierten IP-Pools aufzulisten, die in Ihrem Konto vorhanden sind	List		ses:ApiVersion	
ListDeliverabilityTestReports	Gewährt die Berechtigung zum Abrufen einer Liste der von Ihnen durchgeführten prädiktiven Tests zur Platzierung im Posteingang unabhängig von deren Status	List		ses:ApiVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDomainDeliverabilityCampaigns	Gewährt die Berechtigung zum Abrufen von Zustellbarkeitsdaten für alle Kampagnen, die eine bestimmte Domain zum Senden von E-Mails während eines bestimmten Zeitraums verwendet haben	Read		ses:ApiVersion	
ListEmailIdentities	Gewährt die Berechtigung zum Auflisten aller mit Ihrem Konto verknüpften E-Mail-Id entitäten	List		ses:ApiVersion	
ListTagsForResource	Gewährt die Berechtigung zum Aufrufen einer Liste der Tags (Schlüssel und Werte), die einer bestimmten Ressource zugeordnet sind	Read	configuration-set		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		
				ses:ApiVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutAccountDedicatedIpWarmupAttributes	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren der automatischen Aufwärmfunktion für dedizierte IP-Adressen	Write		ses:ApiVersion	
PutAccountSendingAttributes	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren der Fähigkeit Ihres Kontos, E-Mails zu senden	Write		ses:ApiVersion	
PutConfigurationSetDeliveryOptions	Gewährt die Berechtigung zum Verknüpfen eines Konfigurationssatzes mit einem dedizierten IP-Pool	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetReputationOptions	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren der Sammlung von Zuverlässigkeitsmetriken für E-Mails, die unter Verwendung eines bestimmten Konfigurationssatzes versendet werden	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutConfigurationSetSendingOptions	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren des E-Mail-Versands für Nachrichten, die einen bestimmten Konfigurationssatz verwenden	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetTrackingOptions	Gewährt die Berechtigung zum Angeben einer benutzerdefinierten Domain, die für offene und Klicknachverfolgungs-Elemente in E-Mails verwendet werden soll, die Sie über einen bestimmten Konfigurationssatz versenden	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpInPool	Gewährt die Berechtigung zum Verschieben einer dedizierten IP-Adresse in einen bestehenden dedizierten IP-Pool	Write	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpWarmupAttributes	Gewährt die Berechtigung zum Aktivieren dedizierter IP-Aufwärmattribute	Write		ses:ApiVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutDeliverabilityDashboardOption	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren des Zustellbarkeits-Dashboards	Write		ses:ApiVersion	
PutEmailIdentityDkimAttributes	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren der DKIM-Authentifizierung für eine E-Mail-Identität	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityFeedbackAttributes	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren der Feedback-Weiterleitung für eine Identität	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityMailFromAttributes	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren der benutzerdefinierten „Mail-From“-Domain-Konfiguration für eine E-Mail-Identität	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
SendEmail	Gewährt die Berechtigung zum Senden einer E-Mail	Write	identity*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
TagResource	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Tags (Schlüssel und Werte) zu einer bestimmten Ressource	Markieren	configuration-set		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen eines oder mehrerer Tags (Schlüssel und Werte) von einer bestimmten Ressource	Markieren	configuration-set		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		
				ses:ApiVersion aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateConfigurationSetEventDestination	Gewährt die Berechtigung zum Aktualisieren der Konfiguration eines Ereignisziels für einen Konfigurationssatz	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Von Amazon Pinpoint Email Service definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
configuration-set	`arn:${Partition}:ses:${Region}:${Account}:configuration-set/${ConfigurationSetName}`	aws:ResourceTag/${TagKey}
dedicated-ip-pool	`arn:${Partition}:ses:${Region}:${Account}:dedicated-ip-pool/${DedicatedIPPool}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
deliverability-test-report	`arn:${Partition}:ses:${Region}:${Account}:deliverability-test-report/${ReportId}`	aws:ResourceTag/${TagKey}
identity	`arn:${Partition}:ses:${Region}:${Account}:identity/${IdentityName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Pinpoint Email Service

Amazon Pinpoint Email Service definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung.	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf den Tag-Schlüssel-Wert-Paaren, die an die Ressource angefügt wurden.	Zeichenfolge
aws:TagKeys	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString
ses:ApiVersion	Filtert Aktionen basierend auf der SES-API-Version.	Zeichenfolge
ses:FeedbackAddress	Filtert Aktionen basierend auf der „Return-Path“-Adresse, die festlegt, wohin Unzustellbarkeitsnachrichten und	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
	Beschwerden von der Funktion für E-Mail-Feedback-Weiterleitung gesendet werden	
ses:FromAddress	Filtert Aktionen basierend auf der „Von“-Adresse einer Nachricht	Zeichenfolge
ses:FromDisplayName	Filtert Aktionen basierend auf der „Von“-Adresse, die als Anzeigename einer Nachricht verwendet wird	Zeichenfolge
ses:Recipients	Filtert Aktionen basierend auf den Empfängeradressen einer Nachricht, einschließlich der „An“-, „CC“- und „BCC“-Adressen	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Pinpoint SMS and Voice Service

Amazon Pinpoint SMS and Voice Service (Servicepräfix: `sms-voice`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Pinpoint SMS and Voice Service definierte Aktionen
- Von Amazon Pinpoint SMS und Voice Service definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Pinpoint SMS and Voice Service

Von Amazon Pinpoint SMS and Voice Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateConfigurationSet	Erstellt einen neuen Konfigurationssatz Nachdem Sie den Konfigurationssatz erstellt haben, können Sie ihm mindestens ein Ereignisziel hinzufügen.	Write			
CreateConfigurationSetEventDestination	Erstellen eines neuen Ereignisziel in einem Konfigurationssatz	Write			iam:PassRole
DeleteConfigurationSet	Löscht einen vorhandenen Konfigurationssatz	Write			
DeleteConfigurationSetEventDestination	Löscht ein Ereignisziel in einem Konfigurationssatz	Write			
GetConfigurationSetEventDestinations	Abrufen von Informationen über ein Ereignisziel, einschließlich der Ereignistypen, die ausgewertet werden, des Amazon-Ressourcennamens (ARN) des Ziels und des Namens des Ereignisziels	Read			
ListConfigurationSets	Gibt eine Liste von Konfigurationssätzen zurück. Bei dieser Produktion werden nur die Konfigurationssätze zurückgegeben, die Ihrem Konto in	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	der aktuellen AWS-Region zugeordnet sind.				
SendVoiceMessage	Erstellen einer neuen Sprachnachricht und deren Versand an die Telefonnummer eines Empfängers	Write			
UpdateConfigurationSetEventDestination	Aktualisiert ein Ereignisziel in einem Konfigurationssatz. Ein Ereignisziel ist ein Ort, an dem Sie Informationen zu Ihren Sprachanrufen veröffentlichen. Sie können beispielsweise ein Ereignis für ein Amazon-CloudWatch-Ziel aufzeichnen, wenn ein Aufruf fehlschlägt.	Write			iam:PassRole

Von Amazon Pinpoint SMS und Voice Service definierte Ressourcentypen

Amazon Pinpoint SMS and Voice Service unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf Amazon Pinpoint SMS und Voice Service zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für Amazon Pinpoint SMS and Voice Service

Pinpoint SMS Voice besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Pinpoint SMS Voice V2

Amazon Pinpoint SMS Voice V2 (Servicepräfix: `sms-voice`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Pinpoint SMS Voice V2 definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateOriginationIdentity	Gewährt die Berechtigung zur Zuordnung einer Originationstelefonnummer oder Absender-ID zu einem Pool	Schreiben	Pool*		
			PhoneNumber		
			SenderId		
AssociateProtectConfiguration	Erteilt die Berechtigung, einem Konfigurationssatz eine Schutzkonfiguration zuzuordnen	Schreiben	ConfigurationSet*		
			ProtectConfiguration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateConfigurationSet	Gewährt die Berechtigung zum Erstellen eines Konfigurationssatzes	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreateEventDestination	Gewährt die Berechtigung zum Erstellen eines Ereignisziels in einem Konfigurationssatz	Schreiben	ConfigurationSet*		iam:PassRole
CreateOptOutList	Gewährt die Berechtigung zum Erstellen einer Opt-Out-Liste	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreatePool	Gewährt die Berechtigung zum Erstellen eines Pools	Schreiben	PhoneNumber		sms-voice:TagResource
			SenderId		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateProtectConfiguration	Erteilt die Berechtigung zum Erstellen einer Schutzkonfiguration	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreateRegistration	Gewährt die Berechtigung zum Erstellen einer Registrierung	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreateRegistrationAssociation	Gewährt die Berechtigung zum Zuordnen einer Registrierung mit einer Telefonnummer oder einer anderen Registrierung	Schreiben	Registration* PhoneNumber		
CreateRegistrationAttachment	Gewährt die Berechtigung zum Erstellen eines Registrierungsanhangs	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreateRegistrationVersion	Gewährt die Berechtigung zum Erstellen einer neuen Registrierungsversion	Schreiben	Registration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateVerifiedDestinationNumber	Gewährt die Berechtigung zum Erstellen einer verifizierten Zielnummer	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
DeleteAccountDefaultProtectConfiguration	Erteilt die Berechtigung zum Löschen der Standardschutzkonfiguration des Kontos	Schreiben			
DeleteConfigurationSet	Gewährt die Berechtigung zum Löschen eines Konfigurationssatzes	Schreiben	ConfigurationSet*		
DeleteDefaultMessageType	Gewährt die Berechtigung zum Löschen des Standardnachrichtentyps für einen Konfigurationssatz	Schreiben	ConfigurationSet*		
DeleteDefaultSenderId	Gewährt die Berechtigung zum Löschen der Standard-Sender-ID für einen Konfigurationssatz	Schreiben	ConfigurationSet*		
DeleteEventDestination	Gewährt die Berechtigung zum Löschen eines Ereignisziels in einem Konfigurationssatz	Schreiben	ConfigurationSet*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteKeyword	Gewährt die Berechtigung zum Löschen eines Schlüsselworts für einen Pool oder eine Originationstelefonnummer	Schreiben	PhoneNumber		
			Pool		
DeleteMediaMessageSpendLimitOverride	Erteilt die Erlaubnis, das monatliche Ausgabenlimit für Medienmitteilungen in Ihrem Konto zu löschen	Schreiben			
DeleteOptOutList	Gewährt die Berechtigung zum Löschen einer Opt-Out-Liste	Schreiben	OptOutList*		
DeleteOptedOutNumber	Gewährt die Berechtigung zum Löschen einer Zieltelefonnummer aus einer Opt-Out-Liste	Schreiben	OptOutList*		
DeletePool	Gewährt die Berechtigung zum Löschen eines Pools	Schreiben	Pool*		
DeleteProtectConfiguration	Erteilt die Berechtigung zum Löschen einer Schutzkonfiguration	Schreiben	ProtectConfiguration*		
DeleteRegistration	Gewährt die Berechtigung zum Löschen einer Registrierung	Schreiben	Registration*		
DeleteRegistrationAttachment	Gewährt die Berechtigung zum Löschen eines Registrierungsanhangs	Schreiben	RegistrationAttachment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteRegistrationFieldValue	Gewährt die Berechtigung zum Löschen eines optionalen Registrierungsfeldwerts	Schreiben	Registration*		
DeleteTextMessageSpendLimitOverride	Gewährt die Berechtigung zum Löschen einer Überschreibung für das monatliche Ausgabenlimit für Textnachrichten Ihres Kontos	Schreiben			
DeleteVerifiedDestinationNumber	Gewährt die Berechtigung zum Löschen einer verifizierten Zielnummer	Schreiben	VerifiedDestinationNumber*		
DeleteVoiceMessageSpendLimitOverride	Gewährt die Berechtigung zum Löschen einer Überschreibung für das monatliche Ausgabenlimit für Sprachnachrichten Ihres Kontos	Schreiben			
DescribeAccountAttributes	Gewährt die Berechtigung zum Beschreiben der Attribute Ihres Kontos	Lesen			
DescribeAccountLimits	Gewährt die Berechtigung zum Beschreiben der Service Quotas für Ihr Konto	Lesen			
DescribeConfigurationSets	Gewährt die Berechtigung zum Beschreiben der Konfigurationssätze in Ihrem Konto	Lesen	ConfigurationSet		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeKeywords	Gewährt die Berechtigung zum Beschreiben eines Schlüsselworts für einen Pool oder eine Originationstelefonnummer	Lesen	PhoneNumber		
			Pool		
DescribeOptOutLists	Gewährt die Berechtigung zum Beschreiben der Opt-Out-Listen in Ihrem Konto	Lesen	OptOutList		
DescribeOptedOutNumbers	Gewährt die Berechtigung zum Beschreiben einer Zieltelefonnummer in einer Opt-Out-Liste	Lesen	OptOutList*		
DescribePhoneNumbers	Gewährt die Berechtigung zum Beschreiben der Ursprungsnummern in Ihrem Konto	Lesen	PhoneNumber		
DescribePools	Gewährt die Berechtigung zum Beschreiben der Pools in Ihrem Konto	Lesen	Pool		
DescribeProtectConfigurations	Erteilt die Erlaubnis, die Schutzkonfigurationen in Ihrem Konto zu beschreiben	Lesen	ProtectConfiguration		
DescribeRegistrationAttachments	Gewährt die Berechtigung zum Beschreiben der Registrierungsanhänge in Ihrem Konto	Lesen	RegistrationAttachment		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeRegistrationFieldDefinitions	Gewährt die Berechtigung zum Beschreiben der Felddefinitionen für einen bestimmten Registrierungstyp	Lesen			
DescribeRegistrationFieldValues	Gewährt die Berechtigung zum Beschreiben der Feldwerte für eine bestimmte Registrierung	Lesen	Registration*		
DescribeRegistrationSectionDefinitions	Gewährt die Berechtigung zum Beschreiben der Abschnittsdefinitionen für einen bestimmten Registrierungstyp	Lesen			
DescribeRegistrationTypeDefinitions	Gewährt die Berechtigung zum Beschreiben der vom Service unterstützten Registrierungstypen	Lesen			
DescribeRegistrationVersions	Gewährt die Berechtigung zum Beschreiben der Versionen für eine bestimmte Registrierung	Lesen	Registration*		
DescribeRegistrations	Gewährt die Berechtigung zum Beschreiben der Registrierungen in Ihrem Konto	Lesen	Registration		
DescribeSenderIds	Gewährt die Berechtigung zum Beschreiben der Sender-IDs in Ihrem Konto	Lesen	SenderId		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeSpendLimits	Gewährt die Berechtigung zum Beschreiben der monatlichen Ausgabenlimits für Ihr Konto	Lesen			
DescribeVerifiedDestinationNumbers	Gewährt die Berechtigung zum Beschreiben der verifizierten Zielnummern in Ihrem Konto	Lesen	VerifiedDestinationNumber		
DisassociateOriginationIdentity	Gewährt die Berechtigung zur Trennung der Zuordnung einer Originationstelefonnummer oder Sender-ID zu einem Pool	Schreiben	Pool*		
			PhoneNumber		
			SenderId		
DisassociateProtectConfiguration	Erteilt die Berechtigung, die Zuordnung einer Schutzkonfiguration zu einem Konfigurationssatz aufzuheben	Schreiben	ConfigurationSet*		
			ProtectConfiguration*		
DiscardRegistrationVersion	Gewährt die Berechtigung zum Verwerfen der neuesten Version einer bestimmten Registrierung	Schreiben	Registration*		
GetProtectConfigurationCountryRuleSet	Erteilt die Erlaubnis, den Länderregelsatz für eine Schutzkonfiguration abzurufen	Lesen	ProtectConfiguration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListPoolOriginationIdentities	Gewährt die Berechtigung zur Auflistung aller Originationstelefonnummern oder Sender-IDs zu einem Pool	Lesen	Pool*		
ListRegistrationAssociations	Gewährt die Berechtigung zum Auflisten aller Ressourcen, die einer Registrierung zugeordnet sind	Lesen	Registration*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für eine Ressource	Lesen	ConfigurationSet		
			OptOutList		
			PhoneNumber		
			Pool		
			ProtectConfiguration		
			Registration		
			RegistrationAttachment		
			SenderId		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			VerifiedDestinationNumber		
PutKeyword	Gewährt die Berechtigung zum Erstellen eines Schlüsselworts für einen Pool oder eine Originationstelefonnummer	Schreiben	PhoneNumber		
			Pool		
PutOptedOutNumber	Gewährt die Berechtigung zum Verschieben einer Zieltelefonnummer aus eine Opt-Out-Liste	Schreiben	OptOutList*		
PutRegistrationFieldValue	Gewährt die Berechtigung zum Ablegen eines Registrierungsfeldwerts	Schreiben	Registration*		
ReleasePhoneNumber	Gewährt die Berechtigung zur Freigabe einer Originationstelefonnummer	Schreiben	PhoneNumber*		
ReleaseSenderId	Gewährt die Berechtigung zum Freigeben einer Sender-ID	Schreiben	SenderId*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RequestPhoneNumber	Gewährt die Berechtigung zur Anforderung einer Originationstelefonnummer	Schreiben	Pool		sms-voice:AssociateOriginationIdentity sms-voice:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
RequestSenderId	Gewährt die Berechtigung zum Anfordern einer nicht registrierten Absender-ID	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SendDestinationNumberVerificationCode	Gewährt die Berechtigung zum Senden einer Text- oder Sprachnachricht mit einem Verifizierungscode an eine Zieltelefonnummer	Schreiben	PhoneNumber		sms-voice:SendTextMessage sms-voice:SendVoiceMessage
			Pool		
			SenderId		
SendMediaMessage	Erteilt die Erlaubnis, eine Mediennachricht an eine Zieltelefonnummer zu senden	Schreiben	PhoneNumber		
			Pool		
SendTextMessage	Gewährt die Berechtigung zum Senden einer SMS an eine Zieltelefonnummer	Schreiben	PhoneNumber		
			Pool		
			SenderId		
SendVoiceMessage	Gewährt die Berechtigung zum Senden einer Sprachnachricht an eine Zieltelefonnummer	Schreiben	PhoneNumber		
			Pool		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SetAccountDefaultProtectConfiguration	Erteilt die Berechtigung, eine Standardschutzkonfiguration für das Konto festzulegen	Schreiben	ProtectConfiguration*		
SetDefaultMessageType	Gewährt die Berechtigung zum Festlegen des Standardnachrichttyps für einen Konfigurationssatz	Schreiben	ConfigurationSet*		
SetDefaultSenderId	Gewährt die Berechtigung zum Festlegen der Standard-Sender-ID für einen Konfigurationssatz	Schreiben	ConfigurationSet*		
SetMediaMessageSpendLimitOverride	Erteilt die Erlaubnis, das monatliche Ausgabenlimit für Medienmitteilungen in Ihrem Konto außer Kraft zu setzen	Schreiben			
SetTextMessageSpendLimitOverride	Gewährt die Berechtigung zum Festlegen einer Überschreibung für das monatliche Ausgabenlimit für Textnachrichten Ihres Kontos	Schreiben			
SetVoiceMessageSpendLimitOverride	Gewährt die Berechtigung zum Festlegen einer Überschreibung für das monatliche Ausgabenlimit für Sprachnachrichten Ihres Kontos	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SubmitRegistrationVersion	Gewährt die Berechtigung zum Senden der neuesten Version einer bestimmten Registrierung	Schreiben	Registration*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Ressource	Markieren	ConfigurationSet		
			OptOutList		
			PhoneNumber		
			Pool		
			ProtectConfiguration		
			Registration		
			RegistrationAttachment		
			SenderId		
			VerifiedDestinationNumber		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Ressource	Tagging	ConfigurationSet		
			OptOutList		
			PhoneNumber		
			Pool		
			ProtectConfiguration		
			Registration		
			RegistrationAttachment		
			SenderId		
			VerifiedDestinationNumber		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
UpdateEventDestination	Gewährt die Berechtigung zum Aktualisieren eines Ereignisziels in einem Konfigurationssatz	Schreiben	ConfigurationSet*		iam:PassRole
UpdatePhoneNumber	Gewährt die Berechtigung zum Aktualisieren der Konfiguration einer Originationstelefonnummer	Schreiben	PhoneNumber*		iam:PassRole
UpdatePool	Gewährt die Berechtigung zum Aktualisieren einer Pool-Konfiguration	Schreiben	Pool*		iam:PassRole
UpdateProtectConfiguration	Erteilt die Erlaubnis, eine Schutzkonfiguration zu aktualisieren	Schreiben	ProtectConfiguration*		
UpdateProtectConfigurationCountryRuleSet	Erteilt die Erlaubnis, einen Länderregelsatz für eine Schutzkonfiguration zu aktualisieren	Schreiben	ProtectConfiguration*		
UpdateSenderId	Gewährt die Berechtigung zum Aktualisieren einer ID-Konfiguration	Schreiben	SenderId*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
VerifyDestinationNumber	Gewährt die Berechtigung zur Verifizierung einer Zieltelefonnummer	Schreiben	VerifiedDestinationNumber*		

Von Amazon Pinpoint SMS Voice V2 definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
ConfigurationSet	`arn:${Partition}:sms-voice:${Region}:${Account}:configuration-set/${ConfigurationSetName}`	aws:ResourceTag/${TagKey}
OptOutList	`arn:${Partition}:sms-voice:${Region}:${Account}:opt-out-list/${OptOutListName}`	aws:ResourceTag/${TagKey}
PhoneNumber	`arn:${Partition}:sms-voice:${Region}:${Account}:phone-number/${PhoneNumberId}`	aws:ResourceTag/${TagKey}
Pool	`arn:${Partition}:sms-voice:${Region}:${Account}:pool/${PoolId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
ProtectConfiguration	`arn:${Partition}:sms-voice:${Region}:${Account}:protect-configuration/${ProtectConfigurationId}`	aws:ResourceTag/${TagKey}
SenderId	`arn:${Partition}:sms-voice:${Region}:${Account}:sender-id/${SenderId}/${IsoCountryCode}`	aws:ResourceTag/${TagKey}
Registration	`arn:${Partition}:sms-voice:${Region}:${Account}:registration/${RegistrationId}`	aws:ResourceTag/${TagKey}
RegistrationAttachment	`arn:${Partition}:sms-voice:${Region}:${Account}:registration-attachment/${RegistrationAttachmentId}`	aws:ResourceTag/${TagKey}
VerifiedDestinationNumber	`arn:${Partition}:sms-voice:${Region}:${Account}:verified-destination-number/${VerifiedDestinationNumberId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Pinpoint SMS Voice V2

Amazon Pinpoint SMS Voice V2 definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Polly

Amazon Polly (Servicepräfix: `polly`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Polly definierte Aktionen
- Von Amazon Polly definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Polly

Von Amazon Polly definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteLexicon	Gewährt die Berechtigung zum Löschen des angegeben	Schreiben	lexicon*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	en Aussprachelexikons, das in einer AWS-Region gespeichert ist				
DescribeVoices	Gewährt die Berechtigung zum Beschreiben der Liste der Stimmen, die beim Anfordern der Sprachsynthese zur Verfügung stehen	Auflisten			
GetLexicon	Gewährt die Berechtigung zum Abrufen des Inhalts des angegebenen Aussprachelexikons, das in einer AWS-Region gespeichert ist	Lesen	lexicon*		
GetSpeechSynthesisTask	Gewährt die Berechtigung zum Abrufen von Informationen zu einer bestimmten Sprachsyntheseaufgabe	Lesen			
ListLexicons	Gewährt die Berechtigung zum Auflisten der Aussprachelexika, die in einer AWS-Region gespeichert sind	Auflisten			
ListSpeechSynthesisTasks	Gewährt die Berechtigung zum Auflisten der angeforderten Sprachsyntheseaufgaben	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutLexicon	Gewährt die Berechtigung zum Speichern eines Aussprachelexikons in einer AWS-Region	Schreiben	lexicon*		
StartSpeechSynthesisTask	Gewährt die Berechtigung zum Synthetisieren langer Eingaben für den angegebenen S3-Standort	Schreiben	lexicon		s3:PutObject
SynthesizeSpeech	Gewährt die Berechtigung zum Synthetisieren von Sprache	Lesen	lexicon		

Von Amazon Polly definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
lexicon	`arn:${Partition}:polly:${Region}:${Account}:lexicon/${LexiconName}`	

Bedingungsschlüssel für Amazon Polly

Polly besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Price List

AWS Price List (Servicepräfix: `pricing`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Price List definierte Aktionen
- Von AWS Price List definierte Ressourcentypen
- Bedingungsschlüssel für AWS Price List

Von AWS Price List definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung

mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeServices	Gewährt die Berechtigung zum Abrufen von Servicedetails für alle (paginierten) Services (wenn serviceCode nicht gesetzt ist) oder Servicedetails für einen bestimmten Service (wenn serviceCode angegeben ist)	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAttributeValues	Gewährt die Berechtigung zum Abrufen aller möglichen Werte (paginiert) für ein gegebenen Attribut	Lesen			
GetPriceListFileUrl	Gewährt die Berechtigung zum Abrufen der Preislisten-URL für die angegebenen Parameter	Lesen			
GetProducts	Gewährt die Berechtigung zum Abrufen aller den gegebenen Suchkriterien entsprechenden Produkte	Lesen			
ListPriceLists	Gewährt die Berechtigung zum Auflisten aller (paginierten) in Frage kommenden Preislisten für die angegebenen Parameter	Lesen			

Von AWS Price List definierte Ressourcentypen

AWS Price List unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf AWS Price List zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Price List

Price List besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Private CA Connector for Active Directory

AWS Private CA Connector für Active Directory (Servicepräfix: `pca-connector-ad`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Private CA Connector for Active Directory definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWSzu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateConnector	Gewährt die Berechtigung zum Erstellen eines Connector-Elements in Ihrem Konto	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	acm-pca:DescribeCertificateAuthority acm-pca:GetCertificate acm-pca:G

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					etCertificateAuthorityCertificate acm-pca:IssueCertificate ec2:CreateTags ec2:CreateVpcEndpoint ec2:DescribeVpcEndpoints
CreateDirectoryRegistration	Gewährt die Berechtigung zum Erstellen eines Directory Registration in Ihrem Konto	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	ds:AuthorizeApplication ds:DescribeDirectories
CreateServicePrincipalName	Gewährt die Berechtigung zum Erstellen eines ServicePrincipalName für ein Directory Registration	Schreiben	Directory Registration*		ds:UpdateAuthorizedApplication

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTemplate	Gewährt die Berechtigung zum Erstellen eines Template-Elements für ein Connector-Element	Schreiben	Connector*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTemplateGroupAccessControlEntry	Gewährt die Berechtigung zum Erstellen eines TemplateGroupAccessControlEntry für eine Vorlage	Schreiben	Template*		
DeleteConnector	Gewährt die Berechtigung zum Löschen eines Connector-Elements in Ihrem Konto	Schreiben	Connector*		ec2:DeleteVpcEndpoints ec2:DescribeVpcEndpoints
DeleteDirectoryRegistration	Gewährt die Berechtigung zum Löschen eines Directory Registration in Ihrem Konto	Schreiben	Directory Registration*		ds:UnauthorizeApplication ds:UpdateAuthorizedApplication

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteServicePrincipalName	Gewährt die Berechtigung zum Löschen eines ServicePrincipalName für ein Directory Registration	Schreiben	DirectoryRegistration*		ds:UpdateAuthorizedApplication
DeleteTemplate	Gewährt die Berechtigung zum Löschen eines Template-Elements für ein Connector-Element	Schreiben	Template*		
DeleteTemplateGroupAccessControlEntry	Gewährt die Berechtigung zum Löschen eines TemplateGroupAccessControlEntry für eine Vorlage	Schreiben	Template*		
GetConnector	Gewährt die Berechtigung zum Abrufen eines Connector-Elements in Ihrem Konto	Lesen	Connector*		
GetDirectoryRegistration	Gewährt die Berechtigung zum Abrufen eines Directory Registration in Ihrem Konto	Lesen	DirectoryRegistration*		
GetServicePrincipalName	Gewährt die Berechtigung zum Abrufen eines ServicePrincipalName für ein Directory Registration	Lesen	DirectoryRegistration*		
GetTemplate	Gewährt die Berechtigung zum Abrufen eines Template-Elements für ein Connector-Element	Lesen	Template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetTemplateGroupAccessControlEntry	Gewährt die Berechtigung zum Abrufen eines TemplateGroupAccessControlEntry für eine Vorlage	Lesen	Template*		
ListConnectors	Gewährt die Berechtigung zum Auflisten der Connector-Elemente in Ihrem Konto	Auflisten			
ListDirectoryRegistrations	Gewährt die Berechtigung zum Auflisten der Directory Registrations in Ihrem Konto	Auflisten			
ListServicePrincipalNames	Gewährt die Berechtigung zum Auflisten der ServicePrincipalNames für ein Directory Registration	Auflisten	Directory Registration*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für eine pca-connector-ad Ressource in Ihrem Konto	Lesen			
ListTemplateGroupAccessControlEntries	Gewährt die Berechtigung zum Auflisten der TemplateGroupAccessControlEntries für eine Vorlage	Auflisten	Template*		
ListTemplates	Gewährt die Berechtigung zum Auflisten der Template-Elemente für ein Connector-Element	Auflisten	Connector*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Markieren einer pca-connector-ad Ressource in Ihrem Konto	Tagging	Connector		
			Directory Registration		
			Template		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer pca-connector-ad Ressource in Ihrem Konto	Tagging	Connector		
			Directory Registration		
			Template		
				aws:TagKeys	
UpdateTemplate	Gewährt die Berechtigung zum Aktualisieren eines Template-Elements für ein Connector-Element	Schreiben	Template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateTemplateGroupAccessControlEntry	Gewährt die Berechtigung zum Aktualisieren eines TemplateGroupAccessControlEntry für eine Vorlage	Schreiben	Template*		

Von AWS Private CA Connector for Active Directory definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Connector	`arn:${Partition}:pca-connector-ad:${Region}:${Account}:connector/${ConnectorId}`	aws:ResourceTag/${TagKey}
Directory Registration	`arn:${Partition}:pca-connector-ad:${Region}:${Account}:directory-registration/${DirectoryId}`	aws:ResourceTag/${TagKey}
ServicePrincipalName	`arn:${Partition}:pca-connector-ad:${Region}:${Account}:directory-registration/${DirectoryId}`	
Template	`arn:${Partition}:pca-connector-ad:${Region}:${Account}:connector/${ConnectorId}/template/${TemplateId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
TemplateGroupAccessControlEntry	`arn:${Partition}:pca-connector-ad:${Region}:${Account}:connector/${ConnectorId}/template/${TemplateId}`	

Bedingungsschlüssel für AWS Private CA Connector for Active Directory

AWS Private CA Connector für Active Directory definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach den Tags, die in der Anforderung übergeben werden	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach den Tags, die der Ressource zugeordnet sind	String
aws:TagKeys	Filtert den Zugriff nach den Tag-Schlüsseln, die in der Anforderung übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für die private Zertifizierungsstelle für AWS

Die private Zertifizierungsstelle von AWS (Service-Präfix: `acm-pca`) stellt die folgenden service-spezifischen Ressourcen, Aktionen und Bedingungsschlüssel bereit, die in IAM-Richtlinien verwendet werden können.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von der privaten Zertifizierungsstelle für AWS definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCertificateAuthority	Gewährt die Berechtigung zum Erstellen einer privaten CA für AWS und des zugehörigen privaten Schlüssels und der zugehörigen Konfiguration	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCertificateAuthorityAuditReport	Gewährt die Berechtigung zum Erstellen eines Prüfberichts für eine private CA für AWS	Schreiben	certificate-authority*		
CreatePermission	Gewährt die Berechtigung zum Erstellen einer Berechtigung für eine private CA für AWS	Berechtigungsverwaltung	certificate-authority*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteCertificateAuthority	Gewährt die Berechtigung zum Löschen einer privaten CA für AWS und ihres zugehörigen privaten Schlüssels und ihrer Konfiguration	Schreiben	certificate-authority*		
DeletePermission	Gewährt die Berechtigung zum Löschen einer Berechtigung für eine private CA für AWS	Berechtigungsverwaltung	certificate-authority*		
DeletePolicy	Gewährt die Berechtigung zum Löschen der Richtlinie für eine private CA für AWS	Berechtigungsverwaltung	certificate-authority*		
DescribeCertificateAuthority	Gewährt die Berechtigung, eine Liste der Konfigurations- und Statusfelder zurückzugeben, die in der angegebenen privaten CA für AWS enthalten sind	Lesen	certificate-authority*		
DescribeCertificateAuthorityAuditReport	Gewährt die Berechtigung, den Status und Informationen zu einem Prüfbericht einer privaten CA für AWS zurückzugeben	Lesen	certificate-authority*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetCertificate	Gewährt die Berechtigung zum Abrufen eines privaten CA-Zertifikats für AWS und einer Zertifikatskette für die durch einen ARN angegebene Zertifizierungsstelle	Lesen	certificate-authority*		
GetCertificateAuthorityCertificate	Gewährt die Berechtigung zum Abrufen eines privaten CA-Zertifikats für AWS und einer Zertifikatskette für die durch einen ARN angegebene Zertifizierungsstelle	Lesen	certificate-authority*		
GetCertificateAuthorityCsr	Gewährt die Berechtigung zum Abrufen einer privaten CA-Zertifikatsignieranforderung (CSR) für AWS einer Zertifizierungsstelle für die durch einen ARN angegebene Zertifizierungsstelle	Lesen	certificate-authority*		
GetPolicy	Gewährt die Berechtigung zum Abrufen der Richtlinie auf einer privaten CA für AWS	Lesen	certificate-authority*		
ImportCertificateAuthorityCertificate	Gewährt die Berechtigung zum Importieren eines SSL/TLS-Zertifikats in eine private Zertifizierungsstelle für AWS zur Verwendung als CA-Zertifikat einer privaten CA für AWS	Schreiben	certificate-authority*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
IssueCertificate	Gewährt die Berechtigung zum Ausstellen eines privaten CA-Zertifikats für AWS	Schreiben	certificate-authority*		
				acm-pca:TemplateArn	
ListCertificateAuthorities	Gewährt die Berechtigung zum Abrufen einer Liste der ARNs der privaten CA-Zertifizierungsstelle für AWS und einer Zusammenfassung des Status jeder CA im abrufenden Konto	Auflisten			
ListPermissions	Gewährt die Berechtigung zum Auflisten der Berechtigungen, die auf die private CA-Zertifizierungsstelle für AWS angewendet wurden	Lesen	certificate-authority*		
ListTags	Gewährt die Berechtigung zum Auflisten der Tags, die auf die private CA-Zertifizierungsstelle für AWS angewendet wurden	Lesen	certificate-authority*		
PutPolicy	Gewährt die Berechtigung, einer privaten CA für AWS eine Richtlinie zuzuweisen	Berechtigungsverwaltung	certificate-authority*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RestoreCertificateAuthority	Gewährt die Berechtigung zum Wiederherstellen einer privaten CA für AWS aus dem gelöschten Zustand in den Zustand, in dem sie sich beim Löschen befand	Schreiben	certificate-authority*		
RevokeCertificate	Gewährt die Berechtigung zum Widerrufen eines Zertifikats, das von einer privaten CA für AWS ausgestellt wurde	Schreiben	certificate-authority*		
TagCertificateAuthority	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Tags zu einer privaten CA für AWS	Markierung	certificate-authority*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagCertificateAuthority	Gewährt die Berechtigung zum Entfernen eines oder mehrerer Tags aus einer privaten CA für AWS	Markierung	certificate-authority*		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateCertificateAuthority	Gewährt die Berechtigung zum Aktualisieren der Konfiguration einer privaten CA für AWS	Schreiben	certificate-authority*		

Von der privaten Zertifizierungsstelle für AWS definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
certificate-authority	`arn:${Partition}:acm-pca:${Region}:${Account}:certificate-authority/${CertificateAuthorityId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für die private Zertifizierungsstelle für AWS

Die private Zertifizierungsstelle für AWS definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
acm-pca:TemplateArn	Filtert den Zugriff nach dem ARN der Zertifikatsvorlage, die in der Anfrage zum Ausstellen eines Zertifikats verwendet wurde	ARN
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Proton

AWS Proton (Servicepräfix: `proton`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Proton definierte Aktionen
- Von AWS Proton definierte Ressourcentypen
- Bedingungsschlüssel für AWS Proton

Von AWS Proton definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptEnvironmentAccountConnection	Gewährt die Berechtigung, eine Verbindungsanforderung eines Umgebungskontos von einem anderen Umgebungskonto abzulehnen	Schreiben	environment-account-connection*		
CancelComponentDeployment	Gewährt die Berechtigung zum Abbrechen einer Bereitstellung	Schreiben	component*		
CancelEnvironmentDeployment	Gewährt die Berechtigung zum Abbrechen einer Umgebungsbereitstellung	Write	environment*		
				proton:EnvironmentTemplate	
CancelServiceInstanceDeployment	Gewährt die Berechtigung zum Abbrechen einer Bereitstellung von Service-Instancen	Write	service-instance*		
				proton:ServiceTemplate	
CancelServicePipelineDeployment	Gewährt die Berechtigung zum Abbrechen einer Bereitstellung von Service-Pipelines	Schreiben	service*		
				proton:ServiceTemplate	
CreateComponent	Gewährt die Berechtigung zum Erstellen einer Komponente	Schreiben	component*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEnvironment	Gewährt die Berechtigung zum Erstellen einer Umgebung	Write	environment*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey} proton:EnvironmentTemplate	
CreateEnvironmentAccountConnection	Gewährt die Berechtigung zum Erstellen einer Umgebungskontoverbindung	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateEnvironmentTemplate	Gewährt die Berechtigung zum Erstellen einer Umgebungsvorlage	Schreiben	environment-template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEnvironmentTemplateMajorVersion	Gewährt die Berechtigung zum Erstellen einer Hauptversion einer Umgebungsvorlage VERALTET – Verwenden Sie stattdessen CreateEnvironmentTemplateVersion	Schreiben	environment-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEnvironmentTemplateMinorVersion	Gewährt die Berechtigung zum Erstellen einer Nebenversion einer Umgebungsvorlage VERALTET – Verwenden Sie stattdessen CreateEnvironmentTemplateVersion	Write	environment-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEnvironmentTemplateVersion	Gewährt die Berechtigung zum Erstellen einer Umgebungsvorlage	Schreiben	environment-template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRepository	Gewährt die Berechtigung zum Erstellen eines Repositorys	Schreiben	repository*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateService	Gewährt die Berechtigung zum Erstellen eines Service	Schreiben	service*		codestar-connections:PassConnection
				aws:TagKeys aws:RequestTag/${TagKey} proton:ServiceTemplate	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateServiceInstance	Gewährt die Berechtigung zum Erstellen einer Service-Instance	Schreiben	service-instance*		
				aws:TagKeys aws:RequestTag/${TagKey} proton:ServiceTemplate	
CreateServiceSyncConfig	Gewährt die Berechtigung zum Erstellen einer Service-Synchronisationskonfiguration	Schreiben			
CreateServiceTemplate	Gewährt die Berechtigung zum Erstellen einer Servicevorlage	Schreiben	service-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateServiceTemplateMajorVersion	Gewährt die Berechtigung zum Erstellen einer Hauptversion einer Servicevorlage VERALTET – Verwenden Sie stattdessen CreateServiceTemplateVersion	Schreiben	service-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceTemplateMinorVersion	Gewährt die Berechtigung zum Erstellen einer Nebenversion einer Servicevorlage VERALTET – Verwenden Sie stattdessen CreateServiceTemplateVersion	Write	service-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceTemplateVersion	Gewährt die Berechtigung zum Erstellen einer Servicevorlageversion	Schreiben	service-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateTemplateSyncConfig	Gewährt die Berechtigung zum Erstellen einer Vorlage für die Sync-Konfiguration	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteAccountRoles	Gewährt die Berechtigung zum Löschen der Kontorollen VERALTET – Verwenden Sie stattdessen UpdateAccountSettings	Schreiben			
DeleteComponent	Gewährt die Berechtigung zum Löschen einer Komponente	Schreiben	component*		
DeleteDeployment	Erteilt die Berechtigung zum Löschen einer Bereitstellung	Schreiben	deployment*		
DeleteEnvironment	Gewährt die Berechtigung zum Löschen einer Umgebung	Write	environment*		
				proton:EnvironmentTemplate	
DeleteEnvironmentAccountConnection	Gewährt die Berechtigung zum Löschen einer Umgebungskontoverbindung	Write	environment-account-connection*		
DeleteEnvironmentTemplate	Gewährt die Berechtigung zum Löschen einer Umgebungsvorlage	Schreiben	environment-template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteEnvironmentTemplateMajorVersion	Gewährt die Berechtigung zum Löschen einer Hauptversion einer Umgebungsvorlage VERALTET – Verwenden Sie stattdessen DeleteEnvironmentTemplateVersion	Schreiben	environment-template*		
DeleteEnvironmentTemplateMinorVersion	Gewährt die Berechtigung zum Löschen einer Nebenversion einer Umgebungsvorlage VERALTET – Verwenden Sie stattdessen DeleteEnvironmentTemplateVersion	Write	environment-template*		
DeleteEnvironmentTemplateVersion	Gewährt die Berechtigung zum Löschen einer Umgebungsvorlageversion	Schreiben	environment-template*		
DeleteRepository	Gewährt die Berechtigung zum Löschen eines Repositorys.	Schreiben	repository*		
DeleteService	Gewährt die Berechtigung zum Löschen eines Service	Schreiben	service*		
				proton:ServiceTemplate	
DeleteServiceSyncConfig	Gewährt die Berechtigung zum Löschen einer Service-Synchronisationskonfiguration	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteServiceTemplate	Gewährt die Berechtigung zum Löschen einer Servicevorlage	Schreiben	service-template*		
DeleteServiceTemplateMajorVersion	Gewährt die Berechtigung zum Löschen einer Hauptversion einer Servicevorlage VERALTET – Verwenden Sie stattdessen DeleteServiceTemplateVersion	Schreiben	service-template*		
DeleteServiceTemplateMinorVersion	Gewährt die Berechtigung zum Löschen einer Nebenversion einer Servicevorlage VERALTET – Verwenden Sie stattdessen DeleteServiceTemplateVersion	Write	service-template*		
DeleteServiceTemplateVersion	Gewährt die Berechtigung zum Löschen einer Servicevorlageversion	Schreiben	service-template*		
DeleteTemplateSyncConfig	Gewährt die Berechtigung zum Löschen einer TemplateSyncConfig	Schreiben			
GetAccountRoles	Gewährt die Berechtigung zum Abrufen von Kontorollen VERALTET – Verwenden Sie stattdessen GetAccountSettings	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAccountSettings	Gewährt die Berechtigung zum Beschreiben der Kontoeinstellungen	Lesen			
GetComponent	Gewährt die Berechtigung zum Beschreiben eines Kontakts	Lesen	component*		
GetDeployment	Erteilt die Berechtigung zum Beschreiben einer Bereitstellung	Lesen	deployment*		
GetEnvironment	Gewährt die Berechtigung zum Beschreiben einer Umgebung	Read	environment*		
GetEnvironmentAccountConnection	Gewährt die Berechtigung zum Beschreiben einer Umgebungskontoverbindung	Read	environment-account-connection*		
GetEnvironmentTemplate	Gewährt die Berechtigung zum Beschreiben einer Umgebungsvorlage	Lesen	environment-template*		
GetEnvironmentTemplateMajorVersion	Gewährt die Berechtigung zum Abrufen einer Hauptversion einer Umgebungsvorlage VERALTET – Verwenden Sie stattdessen GetEnvironmentTemplateVersion	Lesen	environment-template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetEnvironmentTemplateMinorVersion	Gewährt die Berechtigung zum Abrufen einer Nebenversion einer Umgebungsvorlage VERALTET – Verwenden Sie stattdessen GetEnvironmentTemplateVersion	Read	environment-template*		
GetEnvironmentTemplateVersion	Gewährt die Berechtigung zum Beschreiben einer Umgebungsvorlageversion	Lesen	environment-template*		
GetRepository	Gewährt die Berechtigung zum Beschreiben eines Repositorys	Lesen	repository*		
GetRepositorySyncStatus	Gewährt die Berechtigung zum Abrufen des neuesten Synchronisierungsstatus für ein Repository	Lesen			
GetResourceTemplateVersionStatusCounts	Gewährt die Berechtigung zum Auflisten des Versionsstatus von Ressourcenvorlagen	Lesen			
GetResourcesSummary	Gewährt die Berechtigung zum Abrufen der Ressourcenzusammenfassung	Lesen			
GetService	Gewährt die Berechtigung zum Beschreiben eines Service	Read	service*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetServiceInstance	Gewährt die Berechtigung zum Beschreiben einer Service-Instance	Lesen	service-instance*		
GetServiceInstanceSyncStatus	Gewährt die Berechtigung zum Beschreiben des Synchronisierungsstatus einer Service-Instance	Lesen			
GetServiceSyncBlockerSummary	Gewährt die Berechtigung zum Beschreiben von Service-Synchronisationssperren für einen Service oder eine Service-Instance	Lesen			
GetServiceSyncConfig	Gewährt die Berechtigung zum Beschreiben einer Service-Synchronisationskonfiguration	Lesen			
GetServiceTemplate	Gewährt die Berechtigung zum Beschreiben einer Servicevorlage	Lesen	service-template*		
GetServiceTemplateMajorVersion	Gewährt die Berechtigung zum Abrufen einer Hauptversion einer Servicevorlage VERALTET – Verwenden Sie stattdessen GetServiceTemplateVersion	Lesen	service-template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetServiceTemplateMinorVersion	Gewährt die Berechtigung zum Abrufen einer Nebenversion einer Servicevorlage VERALTET – Verwenden Sie stattdessen GetServiceTemplateVersion	Read	service-template*		
GetServiceTemplateVersion	Gewährt die Berechtigung zum Beschreiben einer Servicevorlageversion	Lesen	service-template*		
GetTemplateSyncConfig	Gewährt die Berechtigung zum Beschreiben einer TemplateSyncConfig	Lesen			
GetTemplateSyncStatus	Gewährt die Berechtigung zum Beschreiben des Synchronisierungsstatus einer Vorlage	Lesen			
ListComponentOutputs	Gewährt Berechtigung zum Auflisten von Testkomponenten	Auflisten	component*		
			deployment		
ListComponentProvisionedResources	Gewährt die Berechtigung zum Auflisten von Ressourcen, die von der Umgebung bereitgestellt werden	Auflisten	component*		
ListComponents	Gewährt Berechtigung zum Auflisten von Testkomponenten	Auflisten	environment		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			service		
			service-instance		
ListDeployments	Gewährt die Berechtigung zum Auflisten von Bereitstellungen	Auflisten			
ListEnvironmentAccountConnections	Gewährt die Berechtigung, Umgebungskontoverbindungen aufzulisten	Auflisten			
ListEnvironmentOutputs	Gewährt die Berechtigung zum Auflisten von Umgebungsausgaben	Auflisten	environment*		
			deployment		
ListEnvironmentProvisionedResources	Gewährt die Berechtigung zum Auflisten von Ressourcen, die von der Umgebung bereitgestellt werden	Auflisten	environment*		
ListEnvironmentTemplateMajorVersions	Gewährt die Berechtigung zum Auflisten von Hauptversionen einer Umgebungsvorlage VERALTET – Verwenden Sie stattdessen ListenEnvironmentTemplateVersions	Auflisten	environment-template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListEnvironmentTemplateMinorVersions	Gewährt die Berechtigung zum Auflisten einer Nebenversion einer Umgebungsvorlage VERALTET – Verwenden Sie stattdessen ListenEnvironmentTemplateVersions	List	environment-template*		
ListEnvironmentTemplateVersions	Gewährt die Berechtigung zum Auflisten von Umgebungsvorlagenversionen	List	environment-template*		
ListEnvironmentTemplates	Gewährt die Berechtigung zum Auflisten von Umgebungsvorlagen	List			
ListEnvironments	Gewährt die Berechtigung zum Auflisten von Umgebungen	Auflisten			
ListRepositories	Gewährt die Berechtigung zum Auflisten von Repositorys	Auflisten			
ListRepositorySyncDefinitions	Gewährt die Berechtigung zum Auflisten von Sync-Definitionen	Auflisten			
ListServiceInstanceOutputs	Gewährt die Berechtigung zum Auflisten von Service-Instance-Ausgaben	Auflisten	service*		
			service-instance*		
			deployment		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListServiceInstanceProvisionedResources	Gewährt die Berechtigung zum Auflisten von Ressourcen, die von Service-Instances bereitgestellt werden	Auflisten	service*		
			service-instance*		
ListServiceInstances	Gewährt die Berechtigung zum Auflisten von Service-Instances	Auflisten			
ListServicePipelineOutputs	Gewährt die Berechtigung zum Auflisten von Service-Pipeline-Ausgaben	Auflisten	service*		
			deployment		
ListServicePipelineProvisionedResources	Gewährt die Berechtigung zum Auflisten von Ressourcen, die von der Service-Pipeline bereitgestellt werden	Auflisten	service*		
ListServiceTemplateMajorVersions	Gewährt die Berechtigung zum Auflisten von Hauptversionen einer Servicevorlage VERALTET – Verwenden Sie stattdessen ListServiceTemplateVersions	Auflisten	service-template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListServiceTemplateMinorVersions	Gewährt die Berechtigung zum Auflisten von Nebenversionen einer Servicevorlage VERALTET – Verwenden Sie stattdessen ListServiceTemplateVersions	List	service-template*		
ListServiceTemplateVersions	Gewährt die Berechtigung zum Auflisten von Servicevorlagenversionen	List	service-template*		
ListServiceTemplates	Gewährt die Berechtigung zum Auflisten von Servicevorlagen	List			
ListServices	Gewährt die Berechtigung zum Auflisten von Services	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags einer Ressource	Lesen	component		
			environment		
			environment-account-connection		
			environment-template		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			environment-template-major-version		
			environment-template-minor-version		
			environment-template-version		
			repository		
			service		
			service-instance		
			service-template		
			service-template-major-version		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			service-template-minor-version		
			service-template-version		
NotifyResourceDeploymentStatusChange	Gewährt die Berechtigung, Proton über Statusänderungen bei der Ressourcenbereitstellung zu informieren	Schreiben	environment		
			service-instance		
RejectEnvironmentAccountConnection	Gewährt die Berechtigung, eine Verbindungsanforderung eines Umgebungskontos von einem anderen Umgebungskonto abzulehnen	Schreiben	environment-account-connection*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Ressource	Markieren	component		
			environment		
			environment-account-connection		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			environment-template		
			environment-template-major-version		
			environment-template-minor-version		
			environment-template-version		
			repository		
			service		
			service-instance		
			service-template		
			service-template-major-version		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			service-template-minor-version		
			service-template-version		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Ressource	Markierung	component		
			environment		
			environment-account-connection		
			environment-template		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			environment-template-major-version		
			environment-template-minor-version		
			environment-template-version		
			repository		
			service		
			service-instance		
			service-template		
			service-template-major-version		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			service-template-minor-version		
			service-template-version		
				aws:TagKeys	
UpdateAccountRoles	Gewährt die Berechtigung zum Aktualisieren der Kontorollen VERALTET – Verwenden Sie stattdessen UpdateAccountSettings	Write			iam:PassRole
UpdateAccountSettings	Gewährt die Berechtigung zum Aktualisieren der Kontoeinstellungen	Schreiben			iam:PassRole
UpdateComponent	Gewährt die Berechtigung zum Aktualisieren einer Komponente	Schreiben	component*		
UpdateEnvironment	Gewährt die Berechtigung zum Aktualisieren einer Umgebung.	Write	environment*		iam:PassRole
				proton:EnvironmentTemplate	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateEnvironmentAccountConnection	Gewährt die Berechtigung zum Aktualisieren einer Umgebungskontoverbindung	Write	environment-account-connection*		
UpdateEnvironmentTemplate	Gewährt die Berechtigung zum Aktualisieren einer Umgebungsvorlage	Schreiben	environment-template*		
UpdateEnvironmentTemplateMajorVersion	Gewährt die Berechtigung zum Aktualisieren einer Hauptversion einer Umgebungsvorlage VERALTET – Verwenden Sie stattdessen UpdateEnvironmentTemplateVersion	Schreiben	environment-template*		
UpdateEnvironmentTemplateMinorVersion	Gewährt die Berechtigung zum Aktualisieren einer Nebenversion einer Umgebungsvorlage VERALTET – Verwenden Sie stattdessen UpdateEnvironmentTemplateVersion	Write	environment-template*		
UpdateEnvironmentTemplateVersion	Gewährt die Berechtigung zum Aktualisieren von einer Umgebungsvorlagenversion	Write	environment-template*		
UpdateService		Write	service*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Gewährt die Berechtigung zum Aktualisieren eines Service			proton:ServiceTemplate	
UpdateServiceInstance	Gewährt die Berechtigung zum Aktualisieren einer Service-Instance	Write	service-instance*		
				proton:ServiceTemplate	
UpdateServicePipeline	Gewährt die Berechtigung zum Aktualisieren einer Servicepipeline	Schreiben	service*		
				proton:ServiceTemplate	
UpdateServiceSyncBlocker	Gewährt die Berechtigung zum Aktualisieren einer Synchronisationssperre	Schreiben			
UpdateServiceSyncConfig	Gewährt die Berechtigung zum Aktualisieren einer Service-Synchronisationskonfiguration	Schreiben			
UpdateServiceTemplate	Gewährt die Berechtigung zum Aktualisieren einer Servicevorlage	Schreiben	service-template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateServiceTemplateMajorVersion	Gewährt die Berechtigung zum Aktualisieren einer Hauptversion einer Servicevorlage VERALTET – Verwenden Sie stattdessen UpdateServiceTemplateVersion	Schreiben	service-template*		
UpdateServiceTemplateMinorVersion	Gewährt die Berechtigung zum Erstellen einer Nebenversion einer Servicevorlage VERALTET – Verwenden Sie stattdessen UpdateServiceTemplateVersion	Write	service-template*		
UpdateServiceTemplateVersion	Gewährt die Berechtigung zum Aktualisieren einer Servicevorlagenversion	Schreiben	service-template*		
UpdateTemplateSyncConfig	Gewährt die Berechtigung zum Aktualisieren einer TemplateSyncConfig	Schreiben			

Von AWS Proton definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
environment-template	arn:${Partition}:proton:${Region}:${Account}:environment-template/${Name}	aws:ResourceTag/${TagKey}
environment-template-version	arn:${Partition}:proton:${Region}:${Account}:environment-template/${TemplateName}:${MajorVersion}.${MinorVersion}	aws:ResourceTag/${TagKey}
environment-template-major-version	arn:${Partition}:proton:${Region}:${Account}:environment-template/${TemplateName}:${MajorVersionId}	aws:ResourceTag/${TagKey}
environment-template-minor-version	arn:${Partition}:proton:${Region}:${Account}:environment-template/${TemplateName}:${MajorVersionId}.${MinorVersionId}	aws:ResourceTag/${TagKey}
service-template	arn:${Partition}:proton:${Region}:${Account}:service-template/${Name}	aws:ResourceTag/${TagKey}
service-template-version	arn:${Partition}:proton:${Region}:${Account}:service-template/${TemplateName}:${MajorVersion}.${MinorVersion}	aws:ResourceTag/${TagKey}
service-template-major-version	arn:${Partition}:proton:${Region}:${Account}:service-template/${TemplateName}:${MajorVersionId}	aws:ResourceTag/${TagKey}
service-template-minor-version	arn:${Partition}:proton:${Region}:${Account}:service-template/${TemplateName}:${MajorVersionId}.${MinorVersionId}	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
environment	`arn:${Partition}:proton:${Region}:${Account}:environment/${Name}`	aws:ResourceTag/${TagKey}
service	`arn:${Partition}:proton:${Region}:${Account}:service/${Name}`	aws:ResourceTag/${TagKey}
service-instance	`arn:${Partition}:proton:${Region}:${Account}:service/${ServiceName}/service-instance/${Name}`	aws:ResourceTag/${TagKey}
environment-account-connection	`arn:${Partition}:proton:${Region}:${Account}:environment-account-connection/${Id}`	aws:ResourceTag/${TagKey}
repository	`arn:${Partition}:proton:${Region}:${Account}:repository/${Provider}:${Name}`	aws:ResourceTag/${TagKey}
component	`arn:${Partition}:proton:${Region}:${Account}:component/${Id}`	aws:ResourceTag/${TagKey}
deployment	`arn:${Partition}:proton:${Region}:${Account}:deployment/${Id}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Proton

AWS Proton definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert Aktionen nach den Tag-Schlüsseln in der Anforderung	ArrayOfString
proton:EnvironmentTemplate	Filtert Aktionen basierend auf der angegebenen Umgebungsvorlage für Ressource	Zeichenfolge
proton:ServiceTemplate	Filtert Aktionen basierend auf der angegebenen Service-Vorlage im Zusammenhang mit Ressource	Zeichenfolge

Aktionen, Ressourcen und Zustandsschlüssel für AWS Purchase Orders Console

AWS Purchase Orders Console (Servicepräfix: `purchase-orders`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Purchase Orders Console definierte Aktionen

- Von AWS Purchase Orders Console definierte Ressource
- Bedingungsschlüssel für AWS Purchase Orders Console

Von AWS Purchase Orders Console definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddPurchaseOrder [nur Berechtigung]	Gewährt die Berechtigung zum Hinzufügen einer neuen Bestellung	Schreiben	purchase-order*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeletePurchaseOrder [nur Berechtigung]	Gewährt die Berechtigung zum Löschen einer Bestellung	Schreiben	purchase-order*		
				aws:ResourceTag/${TagKey}	
GetConsoleActionSetEnforced [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen, ob vorhandene oder detaillierte IAM-Aktionen verwendet werden, um die Autorisierung für die Fakturierungs-, Kostenmanagement- und Kontokonsolen zu steuern	Lesen			
GetPurchaseOrder [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen einer Bestellung	Lesen	purchase-order*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListPurchaseOrderInvoices [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Bestellrechnungen	Auflisten	purchase-order*		
				aws:ResourceTag/${TagKey}	
ListPurchaseOrders [nur Berechtigung]	Gewährt die Berechtigung, alle Bestellungen für ein Konto aufzulisten	Auflisten			
ListTagsForResource [nur Berechtigung]	Gewährt die Berechtigung, Tags für eine Bestellung aufzulisten	Lesen	purchase-order		
				aws:ResourceTag/${TagKey}	
ModifyPurchaseOrders [nur Berechtigung]	Gewährt die Berechtigung, Bestellungen und deren Details zu ändern	Schreiben	purchase-order*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource [nur Berechtigung]	Gewährt die Berechtigung, Bestellungen mit bestimmten Schlüssel-Wert-Paaren zu taggen	Markierung	purchase-order*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource [nur Berechtigung]	Gewährt die Berechtigung, Tags aus einer Bestellung zu entfernen	Markierung	purchase-order*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateConsoleActionSetEnforced [nur Berechtigung]	Gewährt die Berechtigung zum Ändern, ob vorhandene oder detaillierte IAM-Aktionen verwendet werden sollen, um die Autorisierung für die Fakturierungs-, Kostenmanagement- und Kontokonsolen zu steuern	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdatePurchaseOrder [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren einer vorhandenen Bestellung	Schreiben	purchase-order*		
				aws:ResourceTag/${TagKey}	
UpdatePurchaseOrderStatus [nur Berechtigung]	Gewährt die Berechtigung zum Einrichten eines Bestellstatus	Schreiben	purchase-order*		
				aws:ResourceTag/${TagKey}	
ViewPurchaseOrders [nur Berechtigung]	Gewährt die Berechtigung, Bestellungen und deren Details aufzurufen	Lesen	purchase-order		
				aws:ResourceTag/${TagKey}	

Von AWS Purchase Orders Console definierte Ressource

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
purchase-order	`arn:${Partition}:purchase-orders::${Account}:purchase-order/${ResourceName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Purchase Orders Console

AWS Purchase Orders Console definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Schlüssel eines Tags und den Wert einer Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach den Tag-Schlüsseln in einer Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Q

Amazon Q (Servicepräfix: q) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Q definierte Aktionen
- Von Amazon Q definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Q

Von Amazon Q definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAssignment [nur Berechtigung]	Erteilt die Erlaubnis, eine Benutzer- oder Gruppenzuweisung für ein Amazon Q-Entwicklerprofil zu erstellen	Schreiben			
DeleteAssignment [nur Berechtigung]	Erteilt die Berechtigung zum Löschen einer Benutzer- oder Gruppenzuweisung für ein Amazon Q-Entwicklerprofil	Schreiben			
GetConversation [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen einzelner Nachrichten, die einer bestimmten Konversation mit Amazon Q zugeordnet sind	Lesen			
GetIdentityMetadata [nur Berechtigung]	Erteilt Amazon Q die Erlaubnis, die Identitätsmetadaten abzurufen	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetTroubleshootingResults [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Ergebnissen zur Fehlerbehebung mit Amazon Q	Lesen			
ListConversations [nur Berechtigung]	Erteilt die Erlaubnis, einzelne Konversationen aufzulisten, die mit einem bestimmten Amazon Q-Benutzer verknüpft sind	Lesen			
PassRequest [nur Berechtigung]	Erteilt die Erlaubnis, Amazon Q die Durchführung von Aktionen in Ihrem Namen zu gestatten	Schreiben			
SendMessage [nur Berechtigung]	Gewährt die Berechtigung zum Senden einer Nachricht an Amazon Q	Schreiben			
StartConversation [nur Berechtigung]	Gewährt die Berechtigung zum Starten einer Konversation mit Amazon Q	Schreiben			
StartTroubleshootingAnalysis [nur Berechtigung]	Gewährt die Berechtigung zum Starten einer Analyse zur Fehlerbehebung mit Amazon Q	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartTroubleshootingResolutionExplanation [nur Berechtigung]	Gewährt die Berechtigung zum Starten einer Erläuterung der Problemlösung mit Amazon Q	Schreiben			
UpdateTroubleshootingCommandResult [nur Berechtigung]	Erteilt die Erlaubnis, das Ergebnis eines Befehls zur Fehlerbehebung mit Amazon Q zu aktualisieren	Schreiben			

Von Amazon Q definierte Ressourcentypen

Amazon Q unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf Amazon Q zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für Amazon Q

Q besitzt keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Q Business

Amazon Q Business (Servicepräfix: `qbusiness`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Q Business definierte Aktionen
- Von Amazon Q Business definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Q Business

Von Amazon Q Business definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddUserLicenses	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Benutzer für Lizenzen	Schreiben			
BatchDeleteDocument	Gewährt die Berechtigung für Batch-Löschvorgänge für das Dokument	Schreiben	application*		
			index*		
BatchPutDocument	Gewährt die Berechtigung für Batch-Put-Vorgänge für das Dokument	Schreiben	application*		
			index*		
CancelSubscription	Erteilt die Erlaubnis, ein Abonnement zu kündigen	Schreiben	application*		
			subscription*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Chat	Gewährt die Berechtigung zum Chatten über eine Anwendung	Lesen	application*		
ChatSync	Gewährt die Berechtigung, mithilfe einer Anwendung synchron zu chatten	Lesen	application*		
CreateApplication	Gewährt die Berechtigung zum Erstellen einer Anwendung	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSource	Gewährt die Berechtigung zum Erstellen einer Datenquelle für eine bestimmte Anwendung und einen bestimmten Index	Schreiben	application*		
			index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIndex	Gewährt die Berechtigung zum Erstellen eines Snapshots für eine gegebene Anwendung	Schreiben	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicense	Gewährt die Berechtigung zum Erstellen einer Lizenz	Schreiben			
CreatePlugin	Gewährt die Berechtigung zum Erstellen eines Plugins für eine bestimmte Anwendung	Schreiben	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRetriever	Gewährt die Berechtigung zum Erstellen eines Abrufers für eine bestimmte Anwendung	Schreiben	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscription	Erteilt die Erlaubnis, ein Abonnement zu erstellen	Schreiben	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateUser	Gewährt die Berechtigung zum Erstellen eines Benutzers	Schreiben	application*		
CreateWebExperience	Gewährt die Berechtigung zum Erstellen eines Weberlebnisses für eine bestimmte Anwendung	Schreiben	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Gewährt die Berechtigung zum Löschen einer Anwendung	Schreiben	application*		
DeleteChatControlsConfiguration	Gewährt die Berechtigung zum Löschen einer Chat-Steuerungskonfiguration für eine Anwendung	Schreiben	application*		
DeleteConversation	Gewährt die Berechtigung zum Löschen einer Konversation	Schreiben	application*		
DeleteDataSource	Erteilt die Erlaubnis zum Löschen eines DataSource	Schreiben	application*		
			data-source*		
			index*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteGroup	Gewährt die Berechtigung zum Löschen einer Gruppe	Schreiben	application*		
			index*		
DeleteIndex	Gewährt die Berechtigung zum Löschen eines Index	Schreiben	application*		
			index*		
DeletePlugin	Gewährt die Berechtigung zum Löschen eines Plugins	Schreiben	application*		
			plugin*		
DeleteRetriever	Gewährt die Berechtigung zum Löschen eines Abrufers	Schreiben	application*		
			retriever*		
DeleteUser	Gewährt die Berechtigung zum Löschen eines Benutzers	Schreiben	application*		
DeleteWebExperience	Gewährt die Berechtigung zum Löschen einer Web-Erfahrung	Schreiben	application*		
			web-experience*		
GetApplication	Gewährt die Berechtigung zum Abrufen einer Anwendung	Lesen	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetChatControlsConfiguration	Gewährt die Berechtigung zum Abrufen der Chat-Steuerungskonfiguration für eine Anwendung	Auflisten	application*		
GetDataSource	Gewährt die Berechtigung zum Abrufen einer Datenquelle	Lesen	application*		
			data-source*		
			index*		
GetGroup	Gewährt die Berechtigung zum Abrufen einer Gruppe	Lesen	application*		
			index*		
GetIndex	Gewährt die Berechtigung zum Abrufen eines Index	Lesen	application*		
			index*		
GetLicense	Gewährt die Berechtigung zum Abrufen einer Lizenz	Lesen	user-license*		
GetPlugin	Gewährt die Berechtigung zum Abrufen eines Plugins	Lesen	application*		
			plugin*		
GetRetriever	Gewährt die Berechtigung zum Abrufen eines Abrufers	Lesen	application*		
			retriever*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetUser	Gewährt die Berechtigung zum Abrufen eines Benutzers	Lesen	application*		
GetWebExperience	Gewährt die Berechtigung zum Abrufen einer Web–Erfahrung	Lesen	application*		
			web-experience*		
ListApplications	Gewährt die Berechtigung zum Auflisten von Anwendungen	Auflisten			
ListConversations	Gewährt die Berechtigung zum Auflisten von Konversationen für eine Anwendung	Auflisten	application*		
ListDataSourceSyncJobs	Gewährt die Berechtigung zum Abrufen des Verlaufs von Datenquellen-Synchronisierungsaufgaben	Auflisten	application*		
			data-source*		
			index*		
ListDataSources	Gewährt die Berechtigung zum Auflisten der Datenquellen einer Anwendung und eines Index	Auflisten	application*		
			index*		
ListDocuments	Gewährt die Berechtigung zum Auflisten aller Dokumente	Auflisten	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			index*		
ListGroups	Gewährt die Berechtigung zum Auflisten von Gruppen	Auflisten	application*		
			index*		
ListIndices	Gewährt die Berechtigung zum Auflisten der Indizes einer Anwendung	Auflisten	application*		
ListMessages	Gewährt die Berechtigung zum Auflisten aller Nachrichten	Auflisten	application*		
ListPlugins	Gewährt die Berechtigung zum Auflisten der Plugins einer Anwendung	Auflisten	application*		
ListRetrievers	Gewährt die Berechtigung zum Auflisten der Abrufer einer Anwendung	Auflisten	application*		
ListSubscriptions	Gewährt die Berechtigung zum Auflisten von Abonnements	Auflisten	application*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen	application		
			data-source		
			index		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			plugin		
			retriever		
			web-experience		
ListUserLicenses	Gewährt die Berechtigung zum Auflisten von Lizenzen	Auflisten			
ListWebExperiences	Gewährt die Berechtigung zum Auflisten der Web-Erfahrungen einer Anwendung	Auflisten	application*		
PutFeedback	Gewährt die Berechtigung zum Abgeben eines Feedbacks zu einer Konversationsnachricht	Schreiben	application*		
PutGroup	Gewährt die Berechtigungen zum Abgeben einer Benutzergruppe	Schreiben	application*		
			index*		
RemoveUserLicenses	Gewährt die Berechtigung zum Entfernen von Lizenzen für einen oder mehrere Benutzer	Schreiben			
StartDataSourceSyncJob	Gewährt die Berechtigung zum Starten einer Datenquellen-Synchronisierungsaufgabe	Schreiben	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			data-source*		
			index*		
StopDataSourceSyncJob	Gewährt die Berechtigung zum Anhalten einer Datenquellen-Synchronisierungsaufgabe	Schreiben	application*		
			data-source*		
			index*		
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit bestimmten Schlüsselwertpaaren	Tagging	application		
			data-source		
			index		
			plugin		
			retriever		
			web-experience		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UntagResource	Gewährt die Berechtigung, das Tag mit dem angegebenen Schlüssel aus einer Ressource zu entfernen	Tagging	application		
			data-source		
			index		
			plugin		
			retriever		
			web-experience		
				aws:TagKeys	
UpdateApplication	Gewährt die Berechtigung zum Aktualisieren einer Anwendung	Schreiben	application*		
UpdateChatControlsConfiguration	Gewährt die Berechtigung zum Aktualisieren von Chat-Kontrollkonfigurationen für eine Anwendung	Schreiben	application*		
UpdateDataSource	Erteilt die Erlaubnis zum Aktualisieren eines DataSource	Schreiben	application*		
			data-source*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			index*		
UpdateIndex	Gewährt die Berechtigung zum Aktualisieren eines Index	Schreiben	application*		
			index*		
UpdatePlugin	Gewährt die Berechtigung zum Aktualisieren eines Plugins	Schreiben	application*		
			plugin*		
UpdateRetriever	Gewährt die Berechtigung zum Aktualisieren eines Abrufers	Schreiben	application*		
			retriever*		
UpdateSubscription	Erteilt die Erlaubnis, ein Abonnement zu aktualisieren	Schreiben	application*		
			subscription*		
UpdateUser	Gewährt die Berechtigung zum Aktualisieren eines Benutzers	Schreiben	application*		
UpdateWebExperience	Erteilt die Erlaubnis zum Aktualisieren eines WebExperience	Schreiben	application*		
			web-experience*		

Von Amazon Q Business definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
application	`arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}`	aws:ResourceTag/${TagKey}
retriever	`arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/retriever/${RetrieverId}`	aws:ResourceTag/${TagKey}
index	`arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/index/${IndexId}`	aws:ResourceTag/${TagKey}
data-source	`arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/index/${IndexId}/data-source/${DataSourceId}`	aws:ResourceTag/${TagKey}
plugin	`arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/plugin/${PluginId}`	aws:ResourceTag/${TagKey}
web-experience	`arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/web-experience/${WebExperienceId}`	aws:ResourceTag/${TagKey}

Ressource ntypen	ARN	Bedingungsschlüssel
user-license	`arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/user-license/${UserLicenseId}`	
subscription	`arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/subscription/${SubscriptionId}`	

Bedingungsschlüssel für Amazon Q Business

Amazon Q Business definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Q Business Q Apps

Amazon Q Business Q Apps (Servicepräfix:`qapps`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Q Business Q Apps definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateQAppWithUser [nur Berechtigung]	Erteilt die Erlaubnis, Q App einem Benutzer in der Q Business-Anwendung zuzuordnen	Schreiben	application*		
CopyQApp [nur Berechtigung]	Erteilt die Erlaubnis, Q App in eine Q Business-Anwendung zu kopieren	Schreiben	application*		
CreateLibraryItem [nur Berechtigung]	Erteilt die Erlaubnis, ein Bibliothekselement in einer Q Business-Anwendung zu erstellen	Schreiben	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateLibraryItemReview [nur Berechtigung]	Erteilt die Berechtigung, eine Überprüfung eines Bibliothekselements in einer Q Business-Anwendung zu erstellen	Schreiben	application*		
CreateQApp [nur Berechtigung]	Erteilt die Erlaubnis, eine Q-App in einer Q Business-Anwendung zu erstellen	Schreiben	application*		
CreateSubscriptionToken [nur Berechtigung]	Erteilt die Erlaubnis, ein Q App-Eventbus-Thema in der Q Business-Anwendung zu abonnieren	Schreiben	application*		
DeleteLibraryItem [nur Berechtigung]	Erteilt die Berechtigung zum Löschen eines Bibliothekselements in der Q Business-Anwendung	Schreiben	application*		
DeleteQApp [nur Berechtigung]	Erteilt die Erlaubnis, Q App in einer Q Business-Anwendung zu löschen	Schreiben	application*		
DisassociateQAppFromUser [nur Berechtigung]	Erteilt die Erlaubnis, die Zuordnung von Q App zu einem Benutzer in der Q Business-Anwendung aufzuheben	Schreiben	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetLibraryItem [nur Berechtigung]	Erteilt die Erlaubnis, ein Bibliothekselement in der Q Business-Anwendung abzurufen	Lesen	application*		
GetQApp [nur Berechtigung]	Erteilt die Erlaubnis, Q App in einer Q Business-Anwendung abzurufen	Lesen	application*		
ImportDocumentToQApp [nur Berechtigung]	Erteilt die Erlaubnis, ein Dokument in die Q App in der Q Business-Anwendung zu importieren	Schreiben	application*		
ImportDocumentToQAppSession [nur Berechtigung]	Erteilt die Erlaubnis, ein Dokument in eine Q App-Sitzung in der Q Business-Anwendung zu importieren	Schreiben	application*		
ListLibraryItems [nur Berechtigung]	Erteilt die Erlaubnis, Bibliothekselemente in der Q Business-Anwendung aufzulisten	Auflisten	application*		
ListQApps [nur Berechtigung]	Erteilt die Erlaubnis, Q Apps in einer Q Business-Anwendung aufzulisten	Auflisten	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PredictProblemStatementFromConversation [nur Berechtigung]	Erteilt die Berechtigung, eine Problemstellung anhand des Konversationsprotokolls in der Q Business-Anwendung vorherzusagen	Schreiben	application*		
PredictQAppFromProblemStatement [nur Berechtigung]	Erteilt die Berechtigung, Q App-Metadaten anhand einer Problembeschreibung in der Q Business-Anwendung vorherzusagen	Schreiben	application*		
StartQAppSession [nur Berechtigung]	Erteilt die Erlaubnis, eine Q App-Sitzung in einer Q Business-Anwendung zu starten	Schreiben	application*		
StopQAppSession [nur Berechtigung]	Erteilt die Erlaubnis, die Q App-Sitzung in der Q Business-Anwendung zu beenden	Schreiben	application*		
UpdateLibraryItem [nur Berechtigung]	Erteilt die Erlaubnis, ein Bibliothekselement in der Q Business-Anwendung zu aktualisieren	Schreiben	application*		
UpdateQApp [nur Berechtigung]	Erteilt die Erlaubnis, Q App in einer Q Business-Anwendung zu aktualisieren	Schreiben	application*		

Von Amazon Q Business Q Apps definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
application	`arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}`	

Zustandstasten für Amazon Q Business Q Apps

Q Apps hat keine dienstspezifischen Kontextschlüssel, die im `Condition` Element von Richtlinienerklärungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Q in Connect

Amazon Q in Connect (Servicepräfix: `wisdom`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Q in Connect definierte Aktionen
- Von Amazon Q in Connect definierte Ressourcentypen

- Bedingungsschlüssel für Amazon Q in Connect

Von Amazon Q in Connect definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAssistant	Gewährt die Berechtigung zum Erstellen eines Assistenten	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAssistantAssociation	Gewährt die Berechtigung zum Erstellen einer Verknüpfung zwischen einem Assistenten und einer anderen Ressource	Schreiben	Assistant*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateContent	Gewährt die Berechtigung zum Erstellen von Inhalten	Schreiben	KnowledgeBase*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateContentAssociation	Erteilt die Berechtigung zum Erstellen einer Inhaltsverknüpfung	Schreiben	Content*		
			KnowledgeBase*		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey}	
CreateKnowledgeBase	Gewährt die Berechtigung zum Erstellen einer Wissensdatenbank	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	
CreateQuickResponse	Gewährt die Berechtigung zum Erstellen einer schnellen Reaktion	Schreiben	KnowledgeBase*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateSession	Gewährt die Berechtigung zum Erstellen einer neuen Sitzung	Schreiben	Assistant*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteAssistant	Gewährt die Berechtigung zum Löschen eines Assistenten	Schreiben	Assistant*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteAssistantAssociation	Gewährt die Berechtigung zum Löschen einer Assistentenverbindung	Schreiben	Assistant*		
			AssistantAssociation*		
DeleteContent	Gewährt die Berechtigung zum Löschen von Inhalten	Schreiben	Content*		
			KnowledgeBase*		
DeleteContentAssociation	Erteilt die Berechtigung zum Löschen einer Inhaltsverknüpfung	Schreiben	Content*		
			ContentAssociation*		
			KnowledgeBase*		
DeleteImportJob	Gewährt die Berechtigung zum Löschen eines Importauftrags einer Wissensdatenbank	Schreiben	KnowledgeBase*		
DeleteKnowledgeBase	Gewährt die Berechtigung zum Löschen einer Wissensdatenbank	Schreiben	KnowledgeBase*		
DeleteQuickResponse	Gewährt die Berechtigung zum Löschen einer schnellen Reaktion	Schreiben	KnowledgeBase*		
			QuickResponse*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAssistant	Gewährt die Berechtigung zum Abrufen von Informationen über einen Assistenten	Lesen	Assistant*		
GetAssistantAssociation	Gewährt die Berechtigung zum Abrufen von Informationen über eine Assistentenverbindung	Lesen	Assistant*		
			AssistantAssociation*		
GetContent	Gewährt die Berechtigung zum Abrufen von Inhalten, einschließlich einer vorsignierten URL zum Herunterladen des Inhalts	Lesen	Content*		
			KnowledgeBase*		
GetContentAssociation	Erteilt die Berechtigung zum Abrufen von Informationen über eine Inhaltsverknüpfung	Lesen	Content*		
			ContentAssociation*		
			KnowledgeBase*		
GetContentSummary	Gewährt die Berechtigung zum Abrufen von zusammenfassenden Informationen über die Inhalte	Lesen	Content*		
			KnowledgeBase*		
GetImportJob	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Importauftrag	Lesen	KnowledgeBase*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetKnowledgeBase	Gewährt die Berechtigung zum Abrufen von Informationen über die Wissensdatenbank	Lesen	KnowledgeBase*		
GetQuickResponse	Gewährt die Berechtigung zum Abrufen von Inhalten	Lesen	KnowledgeBase*		
			QuickResponse*		
GetRecommendations	Gewährt die Berechtigung zum Abrufen von Empfehlungen für die angegebene Sitzung	Lesen	Assistant*		
GetSession	Gewährt die Berechtigung zum Abrufen von Informationen für eine angegebene Sitzung	Lesen	Assistant*		
			Session*		
ListAssistantAssociations	Gewährt die Berechtigung zum Auflisten von Informationen über Assistentenverbindungen	Auflisten	Assistant*		
ListAssistants	Gewährt die Berechtigung zum Auflisten von Informationen über Assistenten	Auflisten			
ListContentAssociations	Erteilt die Berechtigung, Informationen über Inhaltszuordnungen aufzulisten	Auflisten	Content*		
			KnowledgeBase*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListContents	Gewährt die Berechtigung zum Auflisten der Inhalte in einer Wissensdatenbank	Auflisten	KnowledgeBase*		
ListImportJobs	Gewährt die Berechtigung zum Auflisten von Informationen über Wissensdatenbanken	Auflisten	KnowledgeBase*		
ListKnowledgeBases	Gewährt die Berechtigung zum Auflisten von Informationen über Wissensdatenbanken	Auflisten			
ListQuickResponses	Gewährt die Berechtigung zum Auflisten der schnellen Reaktion mit einer Wissensdatenbank	Auflisten	KnowledgeBase*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für die angegebene Ressource	Lesen			
NotifyRecommendationsReceived	Gewährt die Berechtigung zum Entfernen der angegebenen Empfehlungen aus der Warteschlange der neu verfügbaren Empfehlungen des angegebenen Assistenten	Schreiben	Assistant*		
PutFeedback	Gewährt die Berechtigung zum Senden von Feedback	Schreiben	Assistant*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
QueryAssistant	Gewährt die Berechtigung zum Durchführen einer manuellen Suche nach dem angegebenen Assistenten	Lesen	Assistant*		
RemoveKnowledgeBaseTemplateUri	Gewährt die Berechtigung zum Entfernen einer URI-Vorlage aus einer Wissensdatenbank	Schreiben	KnowledgeBase*		
SearchContent	Gewährt die Berechtigung zum Suchen nach Inhalten, die auf eine bestimmte Wissensdatenbank verweisen. Kann verwendet werden, um eine bestimmte Inhaltsressource nach ihrem Namen zu finden	Lesen	KnowledgeBase*		
SearchQuickResponses	Gewährt die Berechtigung zum Suchen nach schnellen Reaktionen, die auf eine bestimmte Wissensdatenbank verweisen	Lesen	KnowledgeBase*		wisdom:GetQuickResponse
				wisdom:SearchFilter/RoutingProfileArn	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SearchSessions	Gewährt die Berechtigung zum Suchen nach Sitzungen, die auf einen bestimmten Assistenten verweisen. Kann verwendet werden, um eine bestimmte Sitzungsressource nach ihrem Namen zu finden	Lesen	Assistant*		
StartContentUpload	Gewährt die Berechtigung zum Abrufen einer URL zum Hochladen von Inhalten in eine Wissensdatenbank	Schreiben	KnowledgeBase*		
StartImportJob	Gewährt die Berechtigung zum Erstellen mehrerer schneller Reaktionen	Schreiben	KnowledgeBase*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource	Gewährt die Berechtigung zum Hinzufügen der angegebenen Tags zur angegebenen Ressource	Tagging	Assistant		
			AssistantAssociation		
			Content		
			ContentAssociation		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			Knowledge Base		
			QuickResponse		
			Session		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen der angegebenen Tags aus der angegebenen Ressource	Tagging	Assistant		
			Assistant Association		
			Content		
			ContentAssociation		
			Knowledge Base		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			QuickResponse		
			Session		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateContent	Gewährt die Berechtigung zum Aktualisieren von Informationen über die Inhalte	Schreiben	Content*		
			KnowledgeBase*		
UpdateKnowledgeBaseTemplateUri	Gewährt die Berechtigung zum Aktualisieren einer URI-Vorlage einer Wissensdatenbank	Schreiben	KnowledgeBase*		
UpdateQuickResponse	Gewährt die Berechtigung zum Aktualisieren von Informationen oder Inhalten einer schnellen Reaktion	Schreiben	KnowledgeBase*		
			QuickResponse*		
UpdateSession	Erteilt die Berechtigung zum Aktualisieren einer Sitzung	Schreiben	Assistant*		
			Session*		

Von Amazon Q in Connect definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Assistant	`arn:${Partition}:wisdom:${Region}:${Account}:assistant/${AssistantId}`	aws:ResourceTag/${TagKey}
Assistant Association	`arn:${Partition}:wisdom:${Region}:${Account}:association/${AssistantId}/${AssistantAssociationId}`	aws:ResourceTag/${TagKey}
Content	`arn:${Partition}:wisdom:${Region}:${Account}:content/${KnowledgeBaseId}/${ContentId}`	aws:ResourceTag/${TagKey}
ContentAssociation	`arn:${Partition}:wisdom:${Region}:${Account}:content-association/${KnowledgeBaseId}/${ContentId}/${ContentAssociationId}`	aws:ResourceTag/${TagKey}
Knowledge Base	`arn:${Partition}:wisdom:${Region}:${Account}:knowledge-base/${KnowledgeBaseId}`	aws:ResourceTag/${TagKey}
Session	`arn:${Partition}:wisdom:${Region}:${Account}:session/${AssistantId}/${SessionId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
QuickResponse	`arn:${Partition}:wisdom:${Region}:${Account}:quick-response/${KnowledgeBaseId}/${QuickResponseId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Q in Connect

Amazon Q in Connect definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString
wisdom:SearchFilter/RoutingProfileArn	Filtert den Zugriff nach dem Connect-Routing-Profil-ARN, der in der Anforderung übergeben wird	ARN

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon QLDB

Amazon QLDB (Servicepräfix: `qldb`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon QLDB definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelJournalKinesisStream	Gewährt die Berechtigung zum Abbrechen eines Journalkinesis-Datenstroms.	Write	stream*		
CreateLedger	Gewährt die Berechtigung zum Erstellen eines Ledgers	Write	ledger*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteLedger	Gewährt die Berechtigung zum Löschen eines Ledgers	Write	ledger*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeJournalKinesisStream	Gewährt die Berechtigung zum Beschreiben von Informationen zu einem Journalkinesis-Stream.	Read	stream*		
DescribeJournalS3Export	Gewährt die Berechtigung zum Beschreiben von Informationen zu einem Journalexportauftrag	Read	ledger*		
DescribeLedger	Gewährt die Berechtigung, einen Ledger zu beschreiben	Lesen	ledger*		
ExecuteStatement [nur Berechtigung]	Gewährt die Berechtigung zum Senden von Befehlen an einen Ledger über die Konsole	Write	ledger*		
ExportJournalToS3	Gewährt die Berechtigung zum Exportieren von Journalinhalten in einen Amazon-S3-Bucket	Write	ledger*		
GetBlock	Gewährt die Berechtigung zum Abrufen eines Blocks aus einem Ledger für eine bestimmte BlockAddress	Read	ledger*		
GetDigest	Gewährt die Berechtigung zum Abrufen eines Digest aus einem Ledger für eine bestimmte BlockAddress	Read	ledger*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetRevision	Gewährt die Berechtigung zum Abrufen einer Revision für eine gegebene Dokument-ID und eine gegebene BlockAddress	Lesen	ledger*		
InsertSampleData [nur Berechtigung]	Gewährt die Berechtigung zum Einfügen von Beispielanwendungsdaten über die Konsole	Write	ledger*		
ListJournalKinesisStreamsForLedger	Gewährt die Berechtigung zum Auflisten von Kinesis-Streams für einen bestimmtes Ledger.	List	stream*		
ListJournalS3Exports	Gewährt die Berechtigung zum Auflisten von Journalexportaufträgen für alle Ledger	List			
ListJournalS3ExportsForLedger	Gewährt die Berechtigung zum Auflisten von Journalexportaufträgen für einen bestimmten Ledger	List	ledger*		
ListLedgers	Gewährt die Berechtigung zum Auflisten vorhandener Ledger	List			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Read	catalog		
			ledger		
			stream		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			table		
PartiQLCreateIndex	Gewährt die Berechtigung zum Erstellen eines Index für eine Tabelle	Write	table*		
PartiQLCreateTable	Gewährt die Berechtigung zum Erstellen einer Tabelle.	Write	table*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PartiQLDelete	Gewährt die Berechtigung zum Löschen von Dokumenten aus einer Tabelle	Write	table*		
PartiQLDropIndex	Gewährt die Berechtigung zum Löschen eines Index aus einer Tabelle	Write	table*		
				qldb:Purge	
PartiQLDropTable	Gewährt die Berechtigung zum Ablegen einer Tabelle	Write	table*		
				qldb:Purge	
PartiQLHistoryFunction	Gewährt die Berechtigung zum Verwenden der Verlaufsfunktion für eine Tabelle	Read	table*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PartiQLInsert	Gewährt die Erlaubnis zum Einfügen von Dokumenten in eine Tabelle	Schreiben	table*		
PartiQLRedact	Gewährt die Erlaubnis, historische Überarbeitungen zu redigieren	Schreiben	table*		
PartiQLSelect	Gewährt die Berechtigung zum Auswählen von Dokumenten aus einer Tabelle	Read	catalog		
			table		
PartiQLUndropTable	Gewährt die Berechtigung zum Ausziehen einer Tabelle	Write	table*		
PartiQLUpdate	Gewährt die Berechtigung zum Aktualisieren vorhandener Dokumente in einer Tabelle	Write	table*		
SendCommand	Gewährt die Berechtigung zum Senden von Befehlen an einen Ledger	Schreiben	ledger*		
ShowCatalog [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen eines Ledger-Katalogs über die Konsole	Write	ledger*		
StreamJournalToKinesis	Gewährt die Berechtigung zum Streamen von Journalinhalten in einen Kinesis-Datenstrom.	Write	stream*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Tags zu einer Ressource	Markieren	catalog		
			ledger		
			stream		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung, ein oder mehrere Tags aus einer Ressource zu entfernen	Markieren	catalog		
			ledger		
			stream		
			table		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateLedger	Gewährt die Berechtigung zum Aktualisieren von Eigenschaften in einem Ledger	Write	ledger*		
UpdateLedgerPermissionsMode	Gewährt die Berechtigung zum Aktualisieren des Berechtigungsmodus für ein Ledger	Write	ledger*		

Von Amazon QLDB definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
ledger	`arn:${Partition}:qldb:${Region}:${Account}:ledger/${LedgerName}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
stream	`arn:${Partition}:qldb:${Region}:${Account}:stream/${LedgerName}/${StreamId}`	aws:ResourceTag/${TagKey}
table	`arn:${Partition}:qldb:${Region}:${Account}:ledger/${LedgerName}/table/${TableId}`	aws:ResourceTag/${TagKey}
catalog	`arn:${Partition}:qldb:${Region}:${Account}:ledger/${LedgerName}/information_schema/user_tables`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon QLDB

Amazon QLDB definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wertepaaren, die in der Anforderung zulässig sind	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paar einer Ressource	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach Liste von Tag-Schlüsseln, die in der Anforderung zulässig sind	ArrayOfString

Bedingungsschlüssel	Beschreibung	Typ
qldb:Purge	Filtert den Zugriff nach dem Wert von „purge“, der in einer PartiQL-DROP-Anweisung angegeben ist	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon QuickSight

Amazon QuickSight (Service-Präfix:`quicksight`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon definierte Aktionen QuickSight
- Von Amazon definierte Ressourcentypen QuickSight
- Zustandsschlüssel für Amazon QuickSight

Von Amazon definierte Aktionen QuickSight

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn

die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AccountConfigurations [nur Berechtigung]	Erteilt die Erlaubnis, die Einstellung des Standardzugriffs auf AWS Ressourcen zu aktivieren	Schreiben			
CancelIngestion	Gewährt die Berechtigung zum Abbrechen einer SPICE-Aufnahme für ein Dataset	Schreiben	ingestion*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAccountCustomization	Erteilt die Berechtigung, eine Kontoanpassung für ein QuickSight Konto oder einen Namespace zu erstellen	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAccountSubscription	Erteilt die Erlaubnis zum Abonnieren von QuickSight	Schreiben		quicksight:Edition quicksight:DirectoryType	
CreateAdmin [nur Berechtigung]	Erteilt die Erlaubnis, QuickSight Amazon-Administratoren, Autoren und Leser zur Verfügung zu stellen	Schreiben	user*		
CreateAnalysis	Gewährt die Berechtigung zum Erstellen einer Analyse aus einer Vorlage	Write	analysis*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCustomPermissions [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer benutzerdefinierten Berechtigungsressource zum Einschränken des Benutzerzugriffs	Berechtigungsverwaltung		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDashboard	Erteilt die Erlaubnis, ein QuickSight Dashboard zu erstellen	Schreiben	dashboard*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSet	Gewährt die Berechtigung zum Erstellen eines Dataset	Write	datasource*		quicksight:PassDataSource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSource	Gewährt die Berechtigung zum Erstellen einer Datenquelle	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateEmailCustomizationTemplate [nur Berechtigung]	Erteilt die Erlaubnis, eine QuickSight E-Mail-Anpassungsvorlage zu erstellen	Schreiben	emailCustomizationTemplate*		
CreateFolder	Erteilt die Berechtigung zum Erstellen eines QuickSight Ordners	Schreiben	folder*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFolderMembership	Erteilt die Berechtigung, einem QuickSight Ordner ein QuickSight Dashboard, eine Analyse oder einen Datensatz hinzuzufügen	Schreiben	folder*		
			analysis		
			dashboard		
			dataset		
CreateGroup	Erteilt die Berechtigung zum Erstellen einer QuickSight Gruppe	Schreiben	group*		
CreateGroupMembership	Erteilt die Berechtigung, einen QuickSight Benutzer zu einer QuickSight Gruppe hinzuzufügen	Schreiben	group*	quicksight:UserName	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateIAMPolicyAssignment	Erteilt die Berechtigung, eine Zuweisung mit einem bestimmten IAM-Policy-ARN zu erstellen, die bestimmten Gruppen oder Benutzern von zugewiesen wird QuickSight	Schreiben	assignment*		
CreateIngestion	Gewährt die Berechtigung zum Starten einer SPICE-Aufnahme für ein Dataset	Schreiben	ingestion*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNamespace	Erteilt die Berechtigung zum Erstellen eines Namespaces QuickSight	Schreiben	namespace*		ds:CreateIdentityPoolDirectory
CreateReader [nur Berechtigung]	Erteilt die Erlaubnis zur Bereitstellung von QuickSight Amazon-Lesern	Schreiben	user*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateRefreshSchedule	Gewährt die Berechtigung zum Erstellen eines Aktualisierungszeitplans für einen Datensatz	Schreiben	refreshschedule*		
CreateRoleMembership	Gewährt die Berechtigung zum Hinzufügen eines Gruppenmitglieds zu einer Rolle	Schreiben			
CreateTemplate	Gewährt die Berechtigung zum Erstellen einer Vorlage	Write	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTemplateAlias	Gewährt die Berechtigung zum Erstellen eines Vorlagen-Alias	Schreiben	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTheme	Gewährt die Berechtigung zum Erstellen eines Designs	Schreiben	theme*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateThemeAlias	Gewährt die Berechtigung zum Erstellen eines Alias für eine Designversion	Schreiben	theme*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTopic	Gewährt die Berechtigung zum Erstellen eines Themas	Schreiben	dataset*		quicksight:PassDataSet
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTopicRefreshSchedule	Gewährt die Berechtigung zum Erstellen eines Aktualisierungszeitplans für ein Thema	Schreiben	topic*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateUser [nur Berechtigung]	Erteilt die Erlaubnis, QuickSight Amazon-Autoren und -Leser zur Verfügung zu stellen	Schreiben	user*		
CreateVPCConnection	Gewährt die Berechtigung zum Erstellen einer VPC-Verbindung	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
DeleteAccountCustomization	Erteilt die Erlaubnis, eine Kontoanpassung für ein QuickSight Konto oder einen Namespace zu löschen	Schreiben	customization*		
DeleteAccountSubscription	Erteilt die Berechtigung zum Löschen eines Kontos QuickSight	Schreiben	account*		
DeleteAnalysis	Gewährt die Berechtigung zum Löschen einer Analyse	Schreiben	analysis*		
DeleteCustomPermissions [nur Berechtigung]	Gewährt die Berechtigung zum Löschen einer Ressource für benutzerdefinierte Berechtigungen	Berechtigungsverwaltung			
DeleteDashboard	Erteilt die Erlaubnis zum Löschen eines QuickSight Dashboards	Schreiben	dashboard*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteDataSet	Gewährt die Berechtigung zum Löschen eines Dataset	Schreiben	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDataSetRefreshProperties	Gewährt die Berechtigung zum Löschen von Eigenschaften zur Datensatzaktualisierung für einen Datensatz	Schreiben	dataset*		
DeleteDataSource	Gewährt die Berechtigung zum Löschen einer Datenquelle	Schreiben	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteEmailCustomizationTemplate [nur Berechtigung]	Erteilt die Berechtigung zum Löschen einer QuickSight E-Mail-Anpassungsvorlage	Schreiben	emailCustomizationTemplate*		
DeleteFolder	Erteilt die Berechtigung zum Löschen eines QuickSight Ordners	Schreiben	folder*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteFolderMembership	Erteilt die Berechtigung, ein QuickSight Dashboard, eine Analyse oder einen Datensatz aus einem QuickSight Ordner zu entfernen	Schreiben	folder*		
			analysis		
			dashboard		
			dataset		
DeleteGroup	Erteilt die Berechtigung zum Entfernen einer Benutzergruppe aus QuickSight	Schreiben	group*		
DeleteGroupMembership	Gewährt die Berechtigung zum Entfernen eines Benutzers aus einer Gruppe, sodass er nicht mehr Mitglied der Gruppe ist	Write	group*	quicksight:UserName	
DeleteIAMPolicyAssignment	Gewährt die Berechtigung zum Aktualisieren einer bestehenden Zuweisung	Schreiben	assignment*		
DeleteIdentityPropagationConfig	Erteilt die Berechtigung zum Entfernen von AWS Diensten für die Verbreitung vertrauenswürdiger Identitäten in QuickSight	Schreiben			
DeleteNamespace	Erteilt die Berechtigung zum Löschen eines QuickSight Namespaces	Schreiben	namespace*		ds:DeleteDirectory

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteRefreshSchedule	Gewährt die Berechtigung zum Löschen eines Aktualisierungszeitplans für einen Datensatz	Schreiben	refreshschedule*		
DeleteRoleCustomPermission	Gewährt die Berechtigung zum Entfernen der benutzerdefinierten Berechtigung, die einer Rolle zugeordnet ist	Schreiben			
DeleteRoleMembership	Gewährt die Berechtigung, ein Gruppenmitglied aus einer Rolle zu entfernen	Schreiben			
DeleteTemplate	Gewährt die Berechtigung zum Löschen einer Vorlage	Write	template*		
DeleteTemplateAlias	Gewährt die Berechtigung zum Löschen eines Vorlagen-Alias	Write	template*		
DeleteTheme	Gewährt die Berechtigung zum Löschen eines Designs	Write	theme*		
DeleteThemeAlias	Gewährt die Berechtigung zum Löschen des Alias eines Designs	Schreiben	theme*		
DeleteTopic	Erteilt die Berechtigung zum Löschen eines Themas	Schreiben	topic*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteTopicRefreshSchedule	Gewährt die Berechtigung zum Löschen eines Aktualisierungszeitplans für ein Thema	Schreiben	topic*		
DeleteUser	Erteilt die Berechtigung, einen QuickSight Benutzer unter Angabe des Benutzernamens zu löschen	Schreiben	user*		
DeleteUserByPrincipalId	Gewährt die Berechtigung zum Löschen eines Benutzers, der anhand seiner Prinzipal-ID identifiziert wurde	Schreiben	user*		
DeleteVPCConnection	Gewährt die Berechtigung zum Löschen einer VPC-Verbindung	Schreiben	vpcconnection*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeAccountCustomization	Erteilt die Berechtigung, eine Kontoanpassung für ein QuickSight Konto oder einen Namespace zu beschreiben	Lesen	customization*		
DescribeAccountSettings	Erteilt die Berechtigung, die administrativen Kontoeinstellungen für QuickSight das Konto zu beschreiben	Lesen			
DescribeAccountSubscription	Erteilt die Erlaubnis, ein QuickSight Konto zu beschreiben	Lesen	account*		
DescribeAnalysis	Gewährt die Berechtigung zum Beschreiben einer Analyse	Read	analysis*		
DescribeAnalysisPermissions	Gewährt die Berechtigung zum Beschreiben von Berechtigungen für eine Analyse	Lesen	analysis*		
DescribeAssetBundleExportJob	Gewährt die Berechtigung zum Beschreiben einer Komponenten-Bundle-Exportaufgabe	Lesen	assetBundleExportJob*		
DescribeAssetBundleImportJob	Gewährt die Berechtigung zum Beschreiben einer Komponenten-Bundle-Importaufgabe	Lesen	assetBundleImportJob*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeCustomPermissions [nur Berechtigung]	Erteilt die Erlaubnis, eine benutzerdefinierte Berechtigungsressource in einem QuickSight Konto zu beschreiben	Schreiben			
DescribeDashboard	Erteilt die Erlaubnis, ein QuickSight Dashboard zu beschreiben	Lesen	dashboard*		
DescribeDashboardPermissions	Erteilt die Erlaubnis, Berechtigungen für ein QuickSight Dashboard zu beschreiben	Lesen	dashboard*		
DescribeDashboardSnapshotJob	Gewährt die Berechtigung zum Beschreiben eines Dashboard-Snapshot-Auftrags	Lesen	dashboardSnapshotJob*		
DescribeDashboardSnapshotJobResult	Gewährt die Berechtigung zum Beschreiben des Ergebnisses eines Dashboard-Snapshot-Auftrags	Lesen	dashboardSnapshotJob*		
DescribeDataSet	Gewährt die Berechtigung zum Beschreiben eines Dataset	Read	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDataSetPermissions	Gewährt die Berechtigung zum Beschreiben der Ressourcenrichtlinie eines Dataset	Berechtigungsverwaltung	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeDataSetRefreshProperties	Gewährt die Berechtigung zum Beschreiben von Aktualisierungseigenschaften für einen Datensatz	Lesen	dataset*		
DescribeDataSource	Gewährt die Berechtigung zum Beschreiben einer Datenquelle	Read	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeDataSourcePermissions	Gewährt die Berechtigung zum Beschreiben der Ressourcenrichtlinie einer Datenquelle	Berechtigungsverwaltung	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeEmailCustomizationTemplate [nur Berechtigung]	Erteilt die Erlaubnis, eine QuickSight E-Mail-Anpassungsvorlage zu beschreiben	Lesen	emailCustomizationTemplate*		
DescribeFolder	Erteilt die Erlaubnis, einen QuickSight Ordner zu beschreiben	Lesen	folder*		
DescribeFolderPermissions	Erteilt die Erlaubnis, Berechtigungen für einen QuickSight Ordner zu beschreiben	Lesen	folder*		
DescribeFolderResolvedPermissions	Erteilt die Berechtigung, aufgelöste Berechtigungen für einen QuickSight Ordner zu beschreiben	Lesen	folder*		
DescribeGroup	Erteilt die Erlaubnis, eine QuickSight Gruppe zu beschreiben	Lesen	group*		
DescribeGroupMembership	Erteilt die Erlaubnis, ein QuickSight Gruppenmitglied zu beschreiben	Lesen	group*	quicksight:UserName	
DescribeIAMPolicyAssignment	Gewährt die Berechtigung zum Beschreiben einer vorhandenen Zuweisung	Read	assignment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeIngestion	Gewährt die Berechtigung zum Beschreiben einer SPICE-Aufnahme für ein Dataset	Lesen	ingestion*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeIpRestriction	Erteilt die Erlaubnis, die IP-Einschränkungen für das QuickSight Konto zu beschreiben	Lesen			
DescribeNamespace	Erteilt die Erlaubnis, einen QuickSight Namespace zu beschreiben	Lesen	namespace*		
DescribeRefreshSchedule	Gewährt die Berechtigung zum Beschreiben eines Aktualisierungszeitplans für einen Datensatz	Lesen	refreshschedule*		
DescribeRoleCustomPermission	Gewährt die Berechtigung zum Beschreiben der benutzerdefinierten Berechtigung, die einer Rolle zugeordnet ist	Lesen			
DescribeTemplate	Gewährt die Berechtigung zum Beschreiben einer Vorlage	Read	template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeTemplateAlias	Gewährt die Berechtigung zum Beschreiben eines Vorlagen-Alias	Read	template*		
DescribeTemplatePermissions	Gewährt die Berechtigung zum Beschreiben von Berechtigungen für eine Vorlage	Read	template*		
DescribeTheme	Gewährt die Berechtigung zum Beschreiben eines Designs	Read	theme*		
DescribeThemeAlias	Gewährt die Berechtigung zum Beschreiben eines Design-Alias	Read	theme*		
DescribeThemePermissions	Gewährt die Berechtigung zum Beschreiben von Berechtigungen für ein Design	Lesen	theme*		
DescribeTopic	Gewährt die Berechtigung zum Beschreiben eines Themas	Lesen	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeTopicPermissions	Gewährt die Berechtigung zum Beschreiben der Ressourcenrichtlinie eines Themas	Berechtigungsverwaltung	topic*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeTopicRefresh	Gewährt die Berechtigung zum Beschreiben des Aktualisierungsstatus eines Themas	Lesen	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeTopicRefreshSchedule	Gewährt die Berechtigung zum Beschreiben eines Aktualisierungszeitplans für ein Thema	Lesen	topic*		
DescribeUser	Erteilt die Erlaubnis, einen QuickSight Benutzer anhand des Benutzernamens zu beschreiben	Lesen	user*		
DescribeVPCConnection	Gewährt die Berechtigung zum Beschreiben einer VPC-Verbindung	Lesen	vpcconnection*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
GenerateEmbedUrlForAnonymousUser	Erteilt einem Benutzer, bei dem nicht registriert ist, die Erlaubnis, eine URL zu generieren, die zum Einbetten eines QuickSight Dashboards oder eines Q-Themas verwendet wird QuickSight	Schreiben	namespace*		
			dashboard		
			theme		
			topic		
				aws:TagKeys aws:RequestTag/${TagKey} quicksight:AllowedEmbeddingDomains	
GenerateEmbedUrlForRegisteredUser	Erteilt einem Benutzer, der bei registriert ist, die Erlaubnis, eine URL zu generieren, die zum Einbetten eines QuickSight Dashboards verwendet wird QuickSight	Schreiben	user*		
				quicksight:AllowedEmbeddingDomains	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAnonymousUserEmbedUrl [nur Berechtigung]	Erteilt einem Benutzer, bei dem nicht registriert ist, die Erlaubnis, eine URL abzurufen, die zum Einbetten eines QuickSight Dashboards verwendet wird QuickSight	Lesen			
GetAuthCode [nur Berechtigung]	Erteilt die Erlaubnis, einen Authentifizierungscode abzurufen, der einen QuickSight Benutzer repräsentiert	Lesen	user*		
GetDashboardEmbedUrl	Erteilt die Erlaubnis, eine URL abzurufen, die zum Einbetten eines QuickSight Dashboards verwendet wird	Lesen	dashboard*		
GetGroupMapping [nur Berechtigung]	Erteilt die Erlaubnis QuickSight, Amazon in der Enterprise Edition zu verwenden, um die Microsoft Active Directory-Verzeichnisgruppen (Microsoft Active Directory) zu identifizieren und anzuzeigen, die Rollen in Amazon zugeordnet sind QuickSight	Lesen			
GetSessionEmbedUrl	Erteilt die Erlaubnis, eine URL zum Einbetten der QuickSight Konsolenerfahrung abzurufen	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAnalyses	Gewährt die Berechtigung zum Auflisten aller Analysen in einem Konto	Auflisten	analysis*		
ListAssetBundleExportJobs	Gewährt die Berechtigung zum Auflisten aller Komponenten-Bundle-Exportaufgaben	Auflisten	assetBundleExportJob*		
ListAssetBundleImportJobs	Gewährt die Berechtigung zum Auflisten aller Komponenten-Bundle-Importaufgaben	Auflisten	assetBundleImportJob*		
ListCustomPermissions [nur Berechtigung]	Erteilt die Erlaubnis, Ressourcen mit benutzerdefinierten Berechtigungen im QuickSight Konto aufzulisten	Schreiben			
ListCustomerManagedKeys [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten aller registrierten kundenverwalteten Schlüssel	Auflisten			
ListDashboardVersions	Erteilt die Berechtigung, alle Versionen eines QuickSight Dashboards aufzulisten	Auflisten	dashboard*		
ListDashboards	Erteilt die Berechtigung, alle Dashboards in einem QuickSight Konto aufzulisten	Auflisten	dashboard*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDataSets	Gewährt die Berechtigung zum Auflisten aller Datasets	List		aws:RequestTag/${TagKey} aws:TagKeys	
ListDataSources	Gewährt die Berechtigung zum Auflisten aller Datenquellen	Auflisten		aws:RequestTag/${TagKey} aws:TagKeys	
ListFolderMembers	Gewährt die Berechtigung zum Auflisten aller Raummitglieder.	Lesen	folder*		
ListFolders	Erteilt die Berechtigung, alle Ordner in einem QuickSight Konto aufzulisten	Auflisten	folder*		
ListGroupMemberships	Gewährt die Berechtigung zum Auflisten von Mitgliedsbenutzern in einer Gruppe	Auflisten	group*		
ListGroups	Erteilt die Berechtigung, alle Benutzergruppen aufzulisten in QuickSight	Auflisten	group*		
ListIAMPolicyAssignments	Erteilt die Erlaubnis, alle Aufgaben im aktuellen QuickSight Amazon-Konto aufzulisten	Auflisten	assignment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListIAMPolicyAssignmentsForUser	Gewährt die Berechtigung zum Auflisten aller Zuweisungen, die einem Benutzer zugewiesen sind, sowie der Gruppen, denen er angehört	Auflisten	assignment*		
ListIdentityPropagationConfigs	Erteilt die Erlaubnis, AWS Dienste aufzulisten, die für die Verbreitung vertrauen swürdiger Identitäten aktiviert sind QuickSight	Auflisten			
ListIngestions	Gewährt die Berechtigung zum Auflisten aller SPICE-Aufnahmen für ein Dataset	Auflisten		aws:RequestTag/${TagKey} aws:TagKeys	
ListKMSKeysForUser [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von KMS-Schlüsseln eines Benutzers	Auflisten			
ListNamespaces	Erteilt die Berechtigung, alle Namespaces in einem Konto aufzulisten QuickSight	Auflisten			
ListRefreshSchedules	Gewährt die Berechtigung zum Auflisten aller Aktualisierungszeitpläne für einen Datensatz	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListRoleMemberships	Gewährt die Berechtigung zum Auflisten der Mitglieder einer Rolle	Auflisten			
ListTagsForResource	Erteilt die Berechtigung, Tags einer Ressource aufzulisten QuickSight	Lesen	customization		
			dashboard		
			folder		
			template		
			theme		
			topic		
ListTemplateAliases	Gewährt die Berechtigung zum Auflisten aller Aliasse für eine Vorlage	List	template*		
ListTemplateVersions	Gewährt die Berechtigung zum Auflisten aller Versionen einer Vorlage	Auflisten	template*		
ListTemplates	Erteilt die Erlaubnis, alle Vorlagen in einem QuickSight Konto aufzulisten	Auflisten	template*		
ListThemeAliases	Gewährt die Berechtigung zum Auflisten aller Aliasse eines Designs	List	theme*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListThemeVersions	Gewährt die Berechtigung zum Auflisten aller Versionen eines Designs	List	theme*		
ListThemes	Gewährt die Berechtigung zum Auflisten aller Designs in einem Konto	Auflisten	theme*		
ListTopicRefreshSchedules	Gewährt die Berechtigung zum Auflisten aller Aktualisierungszeitpläne für ein Thema	Auflisten			
ListTopics	Gewährt die Erlaubnis zum Auflisten aller Themen	Auflisten		aws:RequestTag/${TagKey} aws:TagKeys	
ListUserGroups	Gewährt die Berechtigung zum Auflisten der Gruppen, denen ein bestimmter Benutzer angehört	Auflisten	user*		
ListUsers	Erteilt die Berechtigung, alle QuickSight Benutzer aufzulisten, die zu diesem Konto gehören	Auflisten	user*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListVPCConnections	Gewährt die Berechtigung zum Auflisten aller VPC-Verbindungen	Auflisten		aws:RequestTag/${TagKey} aws:TagKeys	
PassDataSet [nur Berechtigung]	Gewährt die Berechtigung zum Verwenden eines Datasets für eine Vorlage	Read	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PassDataSource [nur Berechtigung]	Gewährt die Berechtigung zum Verwenden einer Datenquelle für ein Dataset	Lesen	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutDataSetRefreshProperties	Gewährt die Berechtigung zur Eingabe von Eigenschaften zur Datensatzaktualisierung für einen Datensatz	Schreiben	dataset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RegisterCustomerManagedKey [nur Berechtigung]	Gewährt die Berechtigung zum Registrieren eines kundenverwalteten Schlüssels	Schreiben			
RegisterUser	Erteilt die Berechtigung zum Erstellen eines QuickSight Benutzers, dessen Identität mit der in der Anfrage angegebenen IAM-Identität/Rolle verknüpft ist	Schreiben	user*	quicksight:IamArn quicksight:SessionName	
RemoveCustomerManagedKey [nur Berechtigung]	Gewährt die Berechtigung zum Löschen eines kundenverwalteten Schlüssels	Schreiben			
RestoreAnalysis	Gewährt die Berechtigung zum Wiederherstellen einer gelöschten Analyse	Schreiben	analysis*		
ScopeDownPolicy [nur Berechtigung]	Erteilt die Berechtigung zur Verwaltung von Bereichsrichtlinien für Berechtigungen für Ressourcen AWS	Schreiben			
SearchAnalyses	Gewährt die Berechtigung zum Suchen nach einer Untergruppe von Analysen	Auflisten	analysis*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SearchDashboards	Erteilt die Berechtigung, nach einer Teilmenge von Dashboards zu suchen QuickSight	Auflisten	dashboard*		
SearchDataSets	Erteilt die Berechtigung, nach einer Teilmenge von zu suchen QuickSight DatSets	Auflisten	dataset*		
SearchDataSources	Erteilt die Berechtigung, nach einer Teilmenge von QuickSight Datenquellen zu suchen	Auflisten	datasource*		
SearchDirectoryGroups [nur Berechtigung]	Erteilt die Erlaubnis QuickSight, Amazon in der Enterprise Edition zur Anzeige Ihrer Microsoft Active Directory -Verzeichnisgruppen zu verwenden, sodass Sie auswählen können, welche Gruppen Rollen in Amazon zugeordnet werden sollen QuickSight	Auflisten			
SearchFolders	Erteilt die Berechtigung, nach einer Untergruppe von QuickSight Ordnern zu suchen	Lesen	folder*		
SearchGroups	Erteilt die Berechtigung, nach einer Teilmenge von Gruppen zu suchen QuickSight	Auflisten	group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SearchUsers [nur Berechtigung]	Erteilt die Berechtigung, nach QuickSight Benutzern zu suchen, die zu diesem Konto gehören	Auflisten	user*		
SetGroupMapping [nur Berechtigung]	Erteilt die Erlaubnis QuickSight, Amazon in der Enterprise Edition zur Anzeige Ihrer Microsoft Active Directory -Verzeichnisgruppen zu verwenden, sodass Sie auswählen können, welche Gruppen Rollen in Amazon zugeordnet werden sollen QuickSight	Schreiben			
StartAssetBundleExportJob	Gewährt die Berechtigung zum Starten einer Komponenten-Bundle-Exportaufgabe	Schreiben	assetBundleExportJob*		
StartAssetBundleImportJob	Gewährt die Berechtigung zum Starten einer Komponenten-Bundle-Importaufgabe	Schreiben	assetBundleImportJob*		
StartDashboardSnapshotJob	Gewährt die Berechtigung zum Starten eines Dashboard-Snapshot-Auftrags	Schreiben	dashboardSnapshotJob*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Subscribe [nur Berechtigung]	Erteilt die Erlaubnis QuickSight, Amazon zu abonnieren und dem Benutzer zu ermöglichen, das Abonnement auf die Enterprise Edition zu aktualisieren	Schreiben		quicksight:Edition quicksight:DirectoryType	
TagResource	Erteilt die Erlaubnis, einer QuickSight Ressource Tags hinzuzufügen	Tagging	analysis		
			customization		
			dashboard		
			dataset		
			datasource		
			folder		
			ingestion		
			template		
			theme		
			topic		
			vpcconnection		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
Unsubscribe [nur Berechtigung]	Erteilt die Erlaubnis, sich von Amazon abzumelden QuickSight, wodurch alle Benutzer und ihre Ressourcen dauerhaft von Amazon gelöscht werden QuickSight	Schreiben			
UntagResource	Erteilt die Erlaubnis, Tags aus einer QuickSight Ressource zu entfernen	Tagging	analysis		
			customization		
			dashboard		
			dataset		
			datasource		
			folder		
			ingestion		
			template		
			theme		
			topic		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			vpcconnection		
				aws:TagKeys	
UpdateAccountCustomization	Erteilt die Berechtigung, eine Kontoanpassung für ein QuickSight Konto oder einen Namespace zu aktualisieren	Schreiben	customization*		
UpdateAccountSettings	Erteilt die Berechtigung zum Aktualisieren der Administratorkontoeinstellungen für das QuickSight Konto	Schreiben			
UpdateAnalysis	Gewährt die Berechtigung zum Aktualisieren einer Analyse	Write	analysis*		
UpdateAnalysisPermissions	Gewährt die Berechtigung zum Aktualisieren von Berechtigungen für eine Analyse	Berechtigungsverwaltung	analysis*		
UpdateCustomPermissions [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren einer Ressource für benutzerdefinierte Berechtigungen	Berechtigungsverwaltung			
UpdateDashboard	Erteilt die Erlaubnis, ein QuickSight Dashboard zu aktualisieren	Schreiben	dashboard*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateDashboardLinks	Erteilt die Erlaubnis, die Links eines QuickSight Dashboards zu aktualisieren	Schreiben	dashboard*		
UpdateDashboardPermissions	Erteilt die Erlaubnis, die Berechtigungen für ein QuickSight Dashboard zu aktualisieren	Berechtigungsverwaltung	dashboard*		
UpdateDashboardPublishedVersion	Erteilt die Erlaubnis, die veröffentlichte Version eines QuickSight Dashboards zu aktualisieren	Schreiben	dashboard*		
UpdateDataSet	Gewährt die Berechtigung zum Aktualisieren eines Dataset	Write	dataset*		quicksight:PassDataSource
			datasource		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDataSetPermissions	Gewährt die Berechtigung zum Aktualisieren der Ressourcenrichtlinie eines Dataset	Berechtigungsverwaltung	dataset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDataSource	Gewährt die Berechtigung zum Aktualisieren einer Datenquelle	Write	datasource*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDataSourcePermissions	Gewährt die Berechtigung zum Aktualisieren der Ressourcenrichtlinie einer Datenquelle	Berechtigungsverwaltung	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateEmailCustomizationTemplate [nur Berechtigung]	Erteilt die Erlaubnis, eine QuickSight E-Mail-Anpassungsvorlage zu aktualisieren	Schreiben	emailCustomizationTemplate*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateFolder	Erteilt die Berechtigung zum Aktualisieren eines QuickSight Ordners	Schreiben	folder*		
UpdateFolderPermissions	Erteilt die Berechtigung, die Berechtigungen für einen QuickSight Ordner zu aktualisieren	Berechtigungsverwaltung	folder*		
UpdateGroup	Gewährt die Berechtigung zum Ändern der Gruppenbeschreibung	Write	group*		
UpdateIAMPolicyAssignment	Gewährt die Berechtigung zum Aktualisieren einer bestehenden Zuweisung	Schreiben	assignment*		
UpdateIdentityPropagationConfig	Erteilt die Berechtigung zum Hinzufügen und Aktualisieren von AWS Diensten für die Verbreitung vertrauenswürdiger Identitäten in QuickSight	Schreiben			
UpdateIpRestriction	Erteilt die Erlaubnis, die IP-Einschränkungen für das QuickSight Konto zu aktualisieren	Schreiben			
UpdatePublicSharingSettings	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren der öffentlichen Freigabe für ein Konto	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateRefreshSchedule	Gewährt die Berechtigung zum Aktualisieren eines Aktualisierungszeitplans für einen Datensatz	Schreiben	refreshschedule*		
UpdateResourcePermissions [nur Berechtigung]	Erteilt die Berechtigung zum Aktualisieren von Berechtigungen auf Ressourcenebene in QuickSight	Schreiben			
UpdateRoleCustomPermission	Gewährt die Berechtigung zum Aktualisieren der benutzerdefinierten Berechtigung, die einer Rolle zugeordnet ist	Schreiben			
UpdateSPICECapacityConfiguration	Erteilt die Erlaubnis, die QuickSight SPICE-Kapazitätskonfiguration zu aktualisieren	Schreiben			
UpdateTemplate	Gewährt die Berechtigung zum Aktualisieren einer Vorlage	Write	template*		
UpdateTemplateAlias	Gewährt die Berechtigung zum Aktualisieren eines Vorlagen-Alias	Write	template*		
UpdateTemplatePermissions	Gewährt die Berechtigung zum Aktualisieren von Berechtigungen für eine Vorlage	Berechtigungsverwaltung	template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateTheme	Gewährt die Berechtigung zum Aktualisieren eines Designs	Write	theme*		
UpdateThemeAlias	Gewährt die Berechtigung zum Aktualisieren des Alias eines Designs	Write	theme*		
UpdateThemePermissions	Gewährt die Berechtigung zum Aktualisieren von Berechtigungen für ein Design	Berechtigungsverwaltung	theme*		
UpdateTopic	Gewährt die Berechtigung zum Aktualisieren eines Themas	Schreiben	topic*		quicksight:PassDataSet
			dataset		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTopicPermissions	Gewährt die Berechtigung zum Aktualisieren der Ressourcenrichtlinie eines Themas	Berechtigungsverwaltung	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateTopicRefreshSchedule	Gewährt die Berechtigung zum Aktualisieren eines Aktualisierungszeitplans für ein Thema	Schreiben	topic*		
UpdateUser	Erteilt die Erlaubnis, einen QuickSight Amazon-Benutzer zu aktualisieren	Schreiben	user*		
UpdateVPCConnection	Gewährt die Berechtigung zum Aktualisieren einer VPC-Verbindung	Schreiben	vpcconnection*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	

Von Amazon definierte Ressourcentypen QuickSight

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
account	arn:${Partition}:quicksight:${Region}:${Account}:account/${ResourceId}	
user	arn:${Partition}:quicksight:${Region}:${Account}:user/${ResourceId}	
group	arn:${Partition}:quicksight:${Region}:${Account}:group/${ResourceId}	
analysis	arn:${Partition}:quicksight:${Region}:${Account}:analysis/${ResourceId}	aws:ResourceTag/${TagKey}
dashboard	arn:${Partition}:quicksight:${Region}:${Account}:dashboard/${ResourceId}	aws:ResourceTag/${TagKey}
template	arn:${Partition}:quicksight:${Region}:${Account}:template/${ResourceId}	aws:ResourceTag/${TagKey}
vpcconnection	arn:${Partition}:quicksight:${Region}:${Account}:vpcConnection/${ResourceId}	aws:ResourceTag/${TagKey}
assetBundleExportJob	arn:${Partition}:quicksight:${Region}:${Account}:asset-bundle-export-job/${ResourceId}	
assetBundleImportJob	arn:${Partition}:quicksight:${Region}:${Account}:asset-bundle-import-job/${ResourceId}	
datasource	arn:${Partition}:quicksight:${Region}:${Account}:datasource/${ResourceId}	aws:ResourceTag/${TagKey}
dataset	arn:${Partition}:quicksight:${Region}:${Account}:dataset/${ResourceId}	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
ingestion	arn:${Partition}:quicksight:${Region}:${Account}:dataset/${DatasetId}/ingestion/${ResourceId}	aws:ResourceTag/${TagKey}
refreshschedule	arn:${Partition}:quicksight:${Region}:${Account}:dataset/${DatasetId}/refresh-schedule/${ResourceId}	
theme	arn:${Partition}:quicksight:${Region}:${Account}:theme/${ResourceId}	aws:ResourceTag/${TagKey}
assignment	arn:${Partition}:quicksight::${Account}:assignment/${ResourceId}	
customization	arn:${Partition}:quicksight:${Region}:${Account}:customization/${ResourceId}	aws:ResourceTag/${TagKey}
namespace	arn:${Partition}:quicksight:${Region}:${Account}:namespace/${ResourceId}	
folder	arn:${Partition}:quicksight:${Region}:${Account}:folder/${ResourceId}	aws:ResourceTag/${TagKey}
emailCustomizationTemplate	arn:${Partition}:quicksight:${Region}:${Account}:email-customization-template/${ResourceId}	
topic	arn:${Partition}:quicksight:${Region}:${Account}:topic/${ResourceId}	aws:ResourceTag/${TagKey}
dashboardSnapshotJob	arn:${Partition}:quicksight:${Region}:${Account}:dashboard/${DashboardId}/snapshot-job/${ResourceId}	aws:ResourceTag/${TagKey}

Zustandsschlüssel für Amazon QuickSight

Amazon QuickSight definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach Tag-Schlüsseln	ArrayOfString
quicksight:AllowedEmbeddingDomains	Filtert den Zugriff nach erlaubten Einbettungsdomains	ArrayOfString
quicksight:DirectoryType	Filtert den Zugriff basierend auf den Benutzerverwaltungs-Optionen	String
quicksight:Edition	Filtert den Zugriff nach der Edition von QuickSight	String
quicksight:IamArn	Filtert den Zugriff nach IAM-Benutzer oder Rollen-ARN	ARN
quicksight:SessionName	Filtert den Zugriff nach Sitzungsname	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
quicksight:UserName	Filtert den Zugriff nach Benutzername	String

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon RDS

Amazon RDS (Servicepräfix: `rds`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon RDS definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung

mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddRoleToDBCluster	Gewährt die Berechtigung zum Zuordnen einer Identity and Access Management (IAM)-Rolle von einem Aurora DB-Cluster	Schreiben	cluster*		iam:PassRole
AddRoleToDBInstance	Erteilt die Berechtigung, einer DB-Instance eine AWS Identity and Access	Schreiben	db*		iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Management (IAM) -Rolle zuzuordnen				
AddSourceIdentifierToSubscription	Gewährt die Berechtigung zum Hinzufügen einer Quellkennung zu einem vorhandenen RDS-Ereignisbenachrichtigungsabonnement	Write	es*		
AddTagsToResource	Gewährt die Berechtigung zum Hinzufügen von Metadaten-Tags zu einer Amazon RDS-Ressource	Markieren	cev		
			cluster		
			cluster-endpoint		
			cluster-pg		
			cluster-snapshot		
			db		
			deployment		
			es		
			integration		
			og		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			pg		
			proxy		
			proxy-endpoint		
			ri		
			secgrp		
			snapshot		
			snapshot-tenant-database		
			subgrp		
			target-group		
			tenant-database		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
ApplyPendingMaintenanceAction	Gewährt die Berechtigung zum Anwenden einer ausstehenden Wartungsaktion auf eine Ressource	Schreiben	cluster		
			db		
AuthorizeDBSecurityGroupIngress	Erteilt die Berechtigung, den Zugriff auf eine Datenbank SecurityGroup mithilfe einer von zwei Autorisierungsformen zu ermöglichen	Berechtigungsverwaltung	secgrp*		
BacktrackDBCluster	Gewährt die Berechtigung, einen DB-Cluster bis zu einem bestimmten Zeitpunkt zurückzuverfolgen, ohne einen neuen DB-Cluster zu erstellen	Write	cluster*		
CancelExportTask	Gewährt die Berechtigung zum Abbrechen einer laufenden Exportaufgabe	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CopyDBClusterParameterGroup	Gewährt die Berechtigung zum Kopieren der angegebenen DB-Cluster-Parametergruppe	Write	cluster-pg*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CopyDBClusterSnapshot	Gewährt die Berechtigung zum Erstellen eines Snapshots eines DB-Clusters	Write	cluster-snapshot*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CopyDBParameterGroup	Gewährt die Berechtigung zum Kopieren der angegebenen DB-Parametergruppe	Write	pg*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CopyDBSnapshot	Gewährt die Berechtigung zum Kopieren des angegebenen DB-Snapshots	Write	snapshot*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys rds:CopyOptionGroup	
CopyOptionGroup	Gewährt die Berechtigung zum Kopieren der angegebenen Optionsgruppe	Schreiben	og*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateBlueGreenDeployment	Gewährt die Berechtigung zum Erstellen einer Blau/Grün-Bereitstellung für einen bestimmten Quellcluster oder eine Instance	Schreiben	deployment*		rds:AddTagsToResource rds:CreateDBCluster rds:CreateDBClusterEndpoint rds:CreateDBInstance rds:CreateDBInstanceReadReplica
			cluster		
			cluster-pg		
			db		
			pg		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys rds:cluster-tag/${TagKey} rds:cluster-pg-tag/${TagKey} rds:db-tag/${TagKey} rds:pg-tag/${TagKey} rds:req-tag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				rds:DatabaseEngine rds:DatabaseName rds:StorageEncrypted rds:DatabaseClass rds:StorageSize rds:MultiAz rds:Piops rds:Vpc	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCustomDBEngineVersion	Gewährt die Berechtigung zum Erstellen einer benutzerdefinierten Engine-Version	Schreiben	cev*		iam:CreateServiceLinkedRole mediaimport:CreateDatabaseBinarySnapshot rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDBCluster	Erteilt die Erlaubnis, einen neuen DB-Cluster zu erstellen	Schreiben	cluster*		iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey rds:AddTagsToResource rds:CreateDBInstance secretsmanager:CreateSecret secretsmanager:TagResource
			cluster-pg*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			og*		
			subgrp*		
			db		
			global-cluster		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:DatabaseEngine rds:DatabaseName rds:StorageEncrypted rds:DatabaseClass rds:StorageSize rds:Piops rds:ManageMasterUserPassword	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDBClusterEndpoint	Erteilt die Erlaubnis, einen neuen benutzerdefinierten Endpunkt zu erstellen und ordnet ihn einem Amazon Aurora Aurora-DB-Cluster oder Amazon DocumentDB-Cluster zu	Schreiben	cluster*		rds:AddTagsToResource
			cluster-endpoint*		
				rds:EndpointType aws:RequestTag/${TagKey} aws:TagKeys	
CreateDBClusterParameterGroup	Gewährt die Berechtigung zum Erstellen einer neuen DB-Cluster-Parametergruppe	Write	cluster-pg*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDBClusterSnapshot	Gewährt die Berechtigung zum Erstellen eines Snapshots eines DB-Clusters	Write	cluster*		rds:AddTagsToResource
			cluster-snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDBInstance	Gewährt die Berechtigung zum Erstellen einer neuen DB-Instance	Write	db*		iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey rds:AddTagsToResource rds:CreateTenantDatabase secretsmanager:CreateSecret secretsmanager:TagResource
			cluster		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			og		
			pg		
			secgrp		
			subgrp		
				rds:BackupTarget aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:ManageMasterUserPassword rds:MultiTenant	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDBInstanceReadReplica	Gewährt die Berechtigung zum Erstellen einer DB-Instance, die als Read Replica einer Quell-DB-Instance fungiert	Write	cluster*		iam:PassRole rds:AddTagsToResource
			db*		
			og*		
			pg*		
			subgrp*		
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateDBParameterGroup	Gewährt die Berechtigung zum Erstellen einer neuen DB-Parametergruppe	Write	pg*		rds:AddTagsToResource

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateDBProxy	Gewährt die Berechtigung, einen Datenbank-Proxy zu erstellen	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
CreateDBProxyEndpoint	Gewährt die Berechtigung zum Erstellen eines Datenbank-Proxy-Endpunkts	Write	proxy*		
			proxy-endpoint*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDBSecurityGroup	Gewährt die Berechtigung zum Erstellen einer neuen DB-Sicherheitsgruppe DB-Sicherheitsgruppen steuern den Zugriff auf eine DB-Instance.	Schreiben	secgrp*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateDBShardGroup	Erteilt die Erlaubnis, eine neue Aurora Limitless Database DB-Shard-Gruppe zu erstellen	Schreiben	cluster*		
			shardgrp*		
CreateDBSnapshot	Gewährt die Berechtigung zum Erstellen eines DBSnapshots	Write	db*		rds:AddTagsToResource
			snapshot*		
			snapshot-tenant-database*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				rds:BackupTarget aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateDBSubnetGroup	Gewährt die Berechtigung zum Erstellen einer neuen DB-Subnetzgruppe	Write	subgrp*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateEventSubscription	Gewährt die Berechtigung zum Erstellen eines RDS-Ereignisbenachrichtigungsabonnements	Schreiben	es*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateGlobalCluster	Erteilt die Erlaubnis, eine globale Aurora-Datenbank oder eine globale DocumentDB-Datenbank zu erstellen, die über mehrere Regionen verteilt ist	Schreiben	cluster*		
			global-cluster*		
CreateIntegration	Gewährt die Berechtigung zum Erstellen einer Aurora Null-ETL-Integration mit Redshift	Schreiben	cluster*		kms:CreateGrant kms:DescribeKey rds:AddTagsToResource

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			integration*		
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateOptionGroup	Gewährt die Berechtigung zum Erstellen einer neuen Optionsgruppe	Schreiben	og*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateTenantDatabase	Gewährt Berechtigungen zum Erstellen einer neuen Tenant-Datenbank	Schreiben	db*		rds:AddTagsToResource

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			tenant-database*		
				aws:RequestTag/${TagKey} aws:TagKeys rds:TenantDatabaseName	
CrossRegionCommunication [nur Berechtigung]	Gewährt die Berechtigung für den Zugriff auf eine Ressource in der Remote-Region, wenn regionsübergreifende Produktionen ausgeführt werden, z. B. eine regionsübergreifende Snapshot-Kopie oder eine regionsübergreifende Read Replica-Erstellung	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteBlueGreenDeployment	Gewährt die Berechtigung zum Löschen einer Blau/Grün-Bereitstellung	Schreiben	deployment*		rds:DeleteDBCluster rds:DeleteDBClusterEndpoint rds:DeleteDBInstance
				aws:ResourceTag/${TagKey}	
DeleteCustomDBEngineVersion	Gewährt die Berechtigung zum Löschen einer bestehenden benutzerdefinierten Engine-Version	Schreiben	cev*		
DeleteDBCluster	Gewährt die Berechtigung zum Löschen eines zuvor bereitgestellten DB-Clusters	Schreiben	cluster*		rds:DeleteDBInstance
			cluster-snapshot*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteDBClusterAutomatedBackup	Erteilt die Berechtigung zum Löschen automatisierter Cluster-Backups auf der Grundlage des DbCluster ResourceId Werts des Quell-Clusters oder der Ressourcen-ID des wiederherstellbaren Clusters	Schreiben	cluster-auto-backup*		
DeleteDBClusterEndpoint	Erteilt die Berechtigung zum Löschen eines benutzerdefinierten Endpunkts und entfernt ihn aus einem Amazon Aurora Aurora-DB-Cluster oder Amazon DocumentDB-Cluster	Schreiben	cluster-endpoint*		
DeleteDBClusterParameterGroup	Gewährt die Berechtigung zum Löschen einer angegebenen DB-Cluster-Parametergruppe	Write	cluster-pg*		
DeleteDBClusterSnapshot	Gewährt die Berechtigung zum Löschen eines DB-Cluster-Snapshots	Write	cluster-snapshot*		
DeleteDBInstance	Gewährt die Berechtigung zum Löschen einer zuvor bereitgestellten DB-Instance	Schreiben	db*		rds:DeleteTenantDatabase

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteDBInstanceAutomatedBackup	Erteilt die Erlaubnis, automatische Backups auf der Grundlage des DbiResourceId Werts der Quell-Instance oder der Ressourcen-ID der wiederherstellbaren Instance zu löschen	Schreiben	auto-backup*		
DeleteDBParameterGroup	Erteilt die Berechtigung zum Löschen einer angegebenen Datenbank ParameterGroup	Schreiben	pg*		
DeleteDBProxy	Gewährt die Berechtigung zum Löschen eines Datenbank-Proxys	Write	proxy*		
DeleteDBProxyEndpoint	Gewährt die Berechtigung zum Löschen eines Datenbank-Proxy-Endpunkts	Write	proxy-endpoint*		
DeleteDBSecurityGroup	Gewährt die Berechtigung zum Löschen einer DB-Sicherheitsgruppe	Schreiben	secgrp*		
DeleteDBShardGroup	Erteilt die Berechtigung zum Löschen einer Aurora Limitless Database DB-Shard-Gruppe	Schreiben	shardgrp*		
DeleteDBSnapshot	Gewährt die Berechtigung zum Löschen eines DBSnapshot	Write	snapshot*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteDBSubnetGroup	Gewährt die Berechtigung zum Löschen einer DB-Subnetzgruppe	Write	subgrp*		
DeleteEventSubscription	Gewährt die Berechtigung zum Löschen eines RDS-Ereignisbenachrichtigungsabonnements	Write	es*		
DeleteGlobalCluster	Gewährt die Berechtigung zum Löschen eines globalen Datenbankclusters	Schreiben	global-cluster*		
DeleteIntegration	Gewährt die Berechtigung zum Löschen einer Aurora Null-ETL-Integration mit Redshift	Schreiben	integration*		
DeleteOptionGroup	Gewährt die Berechtigung zum Löschen einer vorhandenen Optionsgruppe	Schreiben	og*		
DeleteTenantDatabase	Gewährt die Berechtigung zum Löschen einer Tenant-Datenbank	Schreiben	db*		
			tenant-database*		
DeregisterDBProxyTargets	Gewährt die Berechtigung, Ziele aus einer Datenbank-Proxy-Zielgruppe zu entfernen	Write	cluster*		
			db*		
			proxy*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			target-group*		
DescribeAccountAttributes	Gewährt die Berechtigung, alle Attribute eines Kundenkontos aufzulisten	Auflisten			
DescribeBlueGreenDeployments	Gewährt die Berechtigung zum Beschreiben von Blau/Grün-Bereitstellungen	Auflisten	deployment		
DescribeCertificates	Erteilt die Erlaubnis, die von Amazon RDS dafür bereitgestellten CA-Zertifikate aufzulisten AWS-Konto	Auflisten			
DescribeDBClusterAutomatedBackups	Erteilt die Berechtigung zum Zurückgeben einer Liste automatisierter Cluster-Sicherungen für aktuelle und gelöschte Cluster	Auflisten	cluster-auto-backup*		
			cluster		
DescribeDBClusterBacktracks	Gewährt die Berechtigung zum Zurückgeben von Informationen über Backtracks für einen DB-Cluster	List	cluster*		
DescribeDBClusterEndpoints	Gewährt die Berechtigung, Informationen zu Endpunkten für einen Amazon Aurora DB-Cluster zurückzugeben	Auflisten	cluster-endpoint*		
			cluster		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDBClusterParameterGroups	Erteilt die Erlaubnis, eine Liste von ClusterParameterGroup DB-Beschreibungen zurückzugeben	Auflisten	cluster-pg*		
DescribeDBClusterParameters	Gewährt die Berechtigung, die detaillierte Parameterliste für eine bestimmte DB-Cluster-Parametergruppe zurückzugeben	List	cluster-pg*		
DescribeDBClusterSnapshotAttributes	Gewährt die Berechtigung, eine Liste der Namen und Werte von DB-Cluster-Attributen eines manuellen DB-Cluster-Snapshots zurückzugeben	List	cluster-snapshot*		
DescribeDBClusterSnapshots	Gewährt die Berechtigung, Informationen über DB-Cluster-Snapshots zurückzugeben	Auflisten	cluster-snapshot*		
DescribeDBClusters	Erteilt die Erlaubnis, Informationen über bereitgestellte Aurora-DB-Cluster oder DocumentDB-Cluster zurückzugeben	Auflisten	cluster*		
DescribeDBEngineVersions	Gewährt die Berechtigung, eine Liste der verfügbaren DB-Engines zurückzugeben	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDBInstanceAutomatedBackups	Gewährt die Berechtigung zum Zurückgeben einer Liste automatisierter Sicherungen für aktuelle und gelöschte Instances	List	auto-backup		
			db		
DescribeDBInstances	Gewährt die Berechtigung zum Rückgeben von Informationen zu bereitgestellten RDS-Instances	List	db*		
DescribeDBLogFiles	Gewährt die Berechtigung, eine Liste von DB-Protokolldateien für die DB-Instance zurückzugeben	Auflisten	db*		
DescribeDBParameterGroups	Erteilt die Erlaubnis, eine Liste mit DB-Beschreibungen zurückzugeben Parameter Group	Auflisten	pg*		
DescribeDBParameters	Gewährt die Berechtigung, die detaillierte Parameterliste für eine bestimmte DB-Parametergruppe zurückzugeben	List	pg*		
DescribeDBProxies	Gewährt die Berechtigung zur Anzeige von Proxys	List	proxy*		
DescribeDBProxyEndpoints	Gewährt die Berechtigung zur Anzeige von Proxy-Endpunkten	List	proxy*		
			proxy-endpoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDBProxyTargetGroups	Gewährt die Berechtigung, Datenbank-Proxy-Zielgruppendetails anzuzeigen	List	proxy*		
DescribeDBProxyTargets	Gewährt die Berechtigung zum Anzeigen von Datenbank-Proxy-Zieldetails	Auflisten	proxy* target-group*		
DescribeDBRecommendations	Gewährt die Berechtigung zum Auflisten von Empfehlungsdetails	Auflisten			
DescribeDBSecurityGroups	Erteilt die Erlaubnis, eine Liste von SecurityGroup DB-Beschreibungen zurückzugeben	Auflisten	secgrp*		
DescribeDBShardGroups	Erteilt die Erlaubnis, Informationen über alle Aurora Limitless Database DB-Shard-Gruppen für dieses Konto zurückzugeben. Sie können nach Shard-Gruppe (n) filtern	Auflisten	shardgrp*		
DescribeDBSnapshotAttributes	Gewährt die Berechtigung, eine Liste der Namen und Werte von DB-Snapshot-Attributen eines manuellen DB-Snapshots zurückzugeben	List	snapshot*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDBSnapshots	Gewährt die Berechtigung zum Zurückgeben von Informationen über DB-Snapshots	Auflisten	snapshot*		
			db		
DescribeDBSubnetGroups	Erteilt die Erlaubnis, eine Liste von SubnetGroup DB-Beschreibungen zurückzugeben	Auflisten	subgrp*		
DescribeDbSnapshotTenantDatabases	Gewährt die Berechtigung zum Zurückgeben von Informationen über Tenant-Datenbanken in DB-Snapshots. Sie können nach Region oder Snapshot filtern	Auflisten	snapshot-tenant-database*		
			db		
			snapshot		
DescribeEngineDefaultClusterParameters	Gewährt die Berechtigung, die Standard-Engine- und System-Parameterinformationen für die Cluster-Datenbank-Engine zurückzugeben	List			
DescribeEngineDefaultParameters	Gewährt die Berechtigung, die Standard-Engine- und System-Parameterinformationen für die angegebene Datenbank-Engine zurückzugeben	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeEventCategories	Gewährt die Berechtigung zum Anzeige einer Liste von Kategorien für alle Ereignisquelltypen oder – falls angegeben – für einen angegebenen Quelltyp	List			
DescribeEventSubscriptions	Gewährt die Berechtigung zum Auflisten aller Abonnementbeschreibungen für ein Kundenkonto	List	es*		
DescribeEvents	Gewährt die Berechtigung, Ereignisse zu DB-Instances, DB-Sicherheitsgruppen, DB-Snapshots und DB-Parametergruppen in den vergangenen 14 Tagen zurückzugeben	List			
DescribeExportTasks	Gewährt die Berechtigung zum Zurückgeben von Informationen zu Exportaufgaben	Auflisten			
DescribeGlobalClusters	Erteilt die Erlaubnis, Informationen über globale Aurora-Datenbankcluster oder globale DocumentDB-Datenbankcluster zurückzugeben	Auflisten	global-cluster*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeIntegrations	Gewährt die Berechtigung zur Beschreibung einer Aurora Null-ETL-Integration mit Redshift	Auflisten	integration*		
				aws:ResourceTag/${TagKey}	
DescribeOptionGroupOptions	Gewährt die Berechtigung zum Beschreiben aller verfügbaren Optionen	List	og*		
DescribeOptionGroups	Gewährt die Berechtigung zum Beschreiben der verfügbaren Optionsgruppen	List	og*		
DescribeOrderableDBInstanceOptions	Gewährt die Berechtigung, eine Liste der bestellbaren DB-Instance-Optionen für die angegebene Engine zurückzugeben	List			
DescribePendingMaintenanceActions	Gewährt die Berechtigung zum Zurückgeben von einer Liste von Ressourcen (z. B. DB-Instances), für die mindestens eine Wartungsaktion aussteht	Auflisten	cluster		
			db		
DescribeRecommendationGroups [nur Berechtigung]	Gewährt die Berechtigung zum Erhalten von Informationen zu Empfehlungsgruppen	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeRecommendations [nur Berechtigung]	Gewährt die Berechtigung zum Erhalten von Informationen zu Empfehlungen	Lesen			
DescribeReservedDBInstances	Gewährt die Berechtigung, Informationen zu reservierten DB-Instances für dieses Konto oder zur angegebenen reservierten DB-Instance zurückzugeben	List	ri*		
DescribeReservedDBInstancesOfferings	Gewährt die Berechtigung, verfügbare reservierte DB-Instance-Angebote aufzulisten	Auflisten			
DescribeSourceRegions	Erteilt die Berechtigung, eine Liste der Quellen zurückzugeben, aus AWS-Regionen der der aktuelle Benutzer eine Read Replica erstellen oder einen DB-Snapshot kopieren AWS-Region kann	Auflisten			
DescribeTenantDatabases	Gewährt die Berechtigung zum Zurückgeben von Informationen über alle bereitgestellten Tenant-Datenbanken. Sie können nach Region oder Snapshot filtern	Auflisten	tenant-database* db		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeValidDBInstanceModifications	Gewährt die Berechtigung zum Auflisten verfügbarer Änderungen, die Sie an Ihrer DB-Instance vornehmen können	Auflisten	db*		
DisableHttpEndpoint	Gewährt die Berechtigung zum Deaktivieren des HTTP-Endpunkts für einen DB-Cluster	Schreiben	cluster*		
DownloadCompleteDBLogFile	Gewährt die Berechtigung zum Herunterladen einer bestimmten Protokolldatei	Lesen	db*		
DownloadDBLogFilePortion	Gewährt die Berechtigung zum Herunterladen der gesamten oder eines Teils der angegebenen Protokolldatei mit einer Größe von bis zu 1 MB	Lesen	db*		
EnableHttpEndpoint	Gewährt die Berechtigung zum Aktivieren des HTTP-Endpunkts für einen DB-Cluster	Schreiben	cluster*		
FailoverDBCluster	Gewährt die Berechtigung zum Erzwingen eines Failovers für einen DB-Cluster	Write	cluster*		
FailoverGlobalCluster		Schreiben	cluster*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Gewährt die Berechtigung zum Failover eines globalen Clusters		global-cluster*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten aller Tags auf einer Amazon RDS-Ressource	Lesen	cev		
			cluster		
			cluster-endpoint		
			cluster-pg		
			cluster-snapshot		
			db		
			es		
			integration		
			og		
			pg		
			proxy		
			proxy-endpoint		
			ri		
			secgrp		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			snapshot		
			snapshot-tenant-database		
			subgrp		
			target-group		
			tenant-database		
ModifyActivityStream	Erteilung der Berechtigung zur Änderung eines Datenbank aktivitätsstroms	Schreiben	db*		
ModifyCertificates	Gewährt die Berechtigung zum Ändern des standardmäßigen SSL/TLS-Zertifikats (Secure Sockets Layer/Transport Layer Security) für Amazon RDS für neue DB-Instances	Schreiben			
ModifyCurrentDBClusterCapacity	Erteilt die Erlaubnis, die aktuelle Clusterkapazität für einen Amazon Aurora Serverless DB-Cluster zu ändern	Schreiben	cluster*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyCustomDBEngineVersion	Gewährt die Berechtigung zum Ändern einer bestehenden benutzerdefinierten Engine-Version	Schreiben	cev*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyDBCluster	Erteilt die Erlaubnis, eine Einstellung für einen Amazon Aurora Aurora-DB-Cluster oder Amazon DocumentDB-Cluster zu ändern	Schreiben	cluster*		iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey rds:ModifyDBInstance secretsmanager:CreateSecret secretsmanager:RotateSecret secretsmanager:TagResource
			cluster-pg*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			og*		
				rds:DatabaseClass rds:StorageSize rds:Piops rds:ManageMasterUserPassword	
ModifyDBClusterEndpoint	Erteilt die Erlaubnis, die Eigenschaften eines Endpunkts in einem Amazon Aurora-DB-Cluster oder Amazon DocumentDB-Cluster zu ändern	Schreiben	cluster-endpoint*		
ModifyDBClusterParameterGroup	Gewährt die Berechtigung zum Ändern der Parameter einer DB-Cluster-Parametergruppe	Write	cluster-pg*		
ModifyDBClusterSnapshotAttribute	Gewährt die Berechtigung zum Hinzufügen eines Attribut und von Werten zu einem manuellen DB-Cluster-Snapshot, oder entfernt ein Attribut und Werte daraus	Write	cluster-snapshot*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyDBInstance	Gewährt die Berechtigung zum Ändern von Einstellungen für eine DB-Instance	Write	db*		iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey rds:AddTagsToResource rds:CreateTenantDatabase secretsmanager:CreateSecret secretsmanager:RotateSecret

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					secretsmanager:TagResource
			og*		
			pg*		
			secgrp*		
				rds:ManageMasterUserPassword rds:MultiTenant	
ModifyDBParameterGroup	Gewährt die Berechtigung zum Ändern der Parameter einer DB-Parametergruppe	Write	pg*		
ModifyDBProxy	Gewährt die Berechtigung, den Datenbank-Proxy zu ändern	Write	proxy*		iam:PassRole
ModifyDBProxyEndpoint	Gewährt die Berechtigung zum Ändern des Datenbank-Proxy-Endpunkts	Write	proxy-endpoint*		
ModifyDBProxyTargetGroup	Gewährt die Berechtigung, die Datenbank-Proxy-Zielgruppe zu ändern	Schreiben	target-group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyDBRecommendation	Gewährt die Berechtigung zum Ändern von Empfehlungen	Schreiben			
ModifyDBShardGroup	Erteilt die Berechtigung, Eigenschaften einer Aurora Limitless Database DB-Shard-Gruppe zu ändern	Schreiben	shardgrp*		
ModifyDBSnapshot	Gewährt die Berechtigung zum Aktualisieren eines manuellen DB-Snapshots, der verschlüsselt oder nicht verschlüsselt sein kann, mit einer neuen Engine-Version	Write	snapshot* og		
ModifyDBSnapshotAttribute	Gewährt die Berechtigung, einem manuellen DB-Snapshot ein Attribut und Werte hinzufügen, oder entfernt ein Attribut und Werte daraus	Write	snapshot*		
ModifyDBSubnetGroup	Gewährt die Berechtigung zum Ändern einer vorhandenen DB-Subnetzgruppe	Write	subgrp*		
ModifyEventSubscription	Gewährt die Berechtigung zum Ändern eines bestehenden RDS-Ereignisbenachrichtigungsabonnements	Schreiben	es*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyGlobalCluster	Erteilt die Erlaubnis, eine Einstellung für einen globalen Amazon Aurora Aurora-Cluster oder einen globalen Amazon DocumentDB-Cluster zu ändern	Schreiben	global-cluster*		
ModifyIntegration	Erteilt die Erlaubnis, eine Aurora Zero-ETL-Integration mit Redshift zu ändern	Schreiben	integration*		
ModifyOptionGroup	Gewährt die Berechtigung zum Ändern einer vorhandenen Optionsgruppe	Schreiben	og*		iam:PassRole
ModifyRecommendation [nur Berechtigung]	Gewährt die Berechtigung zum Ändern von Empfehlungen	Schreiben			
ModifyTenantDatabase	Gewährt die Berechtigung zum Ändern einer Tenant-Datenbank	Schreiben	db*		
			tenant-database*		
				rds:TenantDatabaseName	
PromoteReadReplica	Gewährt die Berechtigung zum Heraufstufen einer Read Replica-DB-Instance auf eine eigenständige DB-Instance	Write	db*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PromoteReadReplicaDBCluster	Gewährt die Berechtigung, einen Read Replica-DB-Cluster auf einen eigenständigen DB-Cluster heraufzustufen	Write	cluster*		
PurchaseReservedDBInstancesOffering	Gewährt die Berechtigung zum Kauf einer reservierten DB-Instance	Schreiben	ri*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RebootDBCluster	Gewährt die Berechtigung zum Neustarten eines zuvor bereitgestellten DB-Clusters	Schreiben	cluster*		rds:RebootDBInstance
RebootDBInstance	Gewährt die Berechtigung zum Neustart des Datenbank-Engine-Service	Schreiben	db*		
RebootDBShardGroup	Erteilt die Erlaubnis, eine Aurora Limitless Database DB-Shard-Gruppe neu zu starten	Schreiben	shardgrp*		
RegisterDBProxyTargets	Gewährt die Berechtigung zum Hinzufügen von Zielen zu einer Datenbank-Proxy-Zielgruppe	Schreiben	target-group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RemoveFromGlobalCluster	Erteilt die Erlaubnis, einen sekundären Aurora-Cluster von einem globalen Aurora-Datenbankcluster oder einem globalen DocumentDB-Cluster zu trennen	Schreiben	cluster*		
			global-cluster*		
RemoveRoleFromDBCluster	Erteilt die Erlaubnis, eine AWS Identity and Access Management (IAM) -Rolle von einem Amazon Aurora Aurora-DB-Cluster zu trennen	Schreiben	cluster*		iam:PassRole
RemoveRoleFromDBInstance	Erteilt die Berechtigung, eine AWS Identity and Access Management (IAM) -Rolle von einer DB-Instance zu trennen	Schreiben	db*		iam:PassRole
RemoveSourceIdentifierFromSubscription	Gewährt die Berechtigung zum Entfernen einer Quellkennung aus einem vorhandenen RDS-Ereignisbenachrichtigungsabonnement	Write	es*		
RemoveTagsFromResource	Gewährt die Berechtigung zum Entfernen von Metadaten tags aus einer Amazon RDS-Ressource	Markieren	cev		
			cluster		
			cluster-endpoint		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			cluster-pg		
			cluster-snapshot		
			db		
			deployment		
			es		
			integration		
			og		
			pg		
			proxy		
			proxy-endpoint		
			ri		
			secgrp		
			snapshot		
			snapshot-tenant-database		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			subgrp		
			target-group		
			tenant-database		
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
ResetDBClusterParameterGroup	Gewährt die Berechtigung zum Ändern der Parameter einer DB-Cluster-Parametergruppe auf den Standardwert	Write	cluster-pg*		
ResetDBParameterGroup	Gewährt die Berechtigung, die Parameter einer DB-Parametergruppe auf die Standardwerte der Engine/des Systems zurückzusetzen	Write	pg*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RestoreDBClusterFromS3	Gewährt die Berechtigung zum Erstellen eines Amazon Aurora DB-Clusters aus Daten, die in einem Amazon S3 Bucket gespeichert sind	Write	cluster*		iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey rds:AddTagsToResource secretsmanager:CreateSecret secretsmanager:TagResource
			cluster-pg*		
			og*		
			subgrp*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:DatabaseEngine rds:DatabaseName rds:StorageEncrypted rds:ManageMasterUserPassword	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RestoreDBClusterFromSnapshot	Gewährt die Berechtigung zum Erstellen eines neuen DB-Clusters aus einem DB-Cluster-Snapshot	Write	cluster*		iam:PassRole rds:AddTagsToResource rds:CreateDBInstance
			cluster-pg*		
			cluster-snapshot*		
			og*		
			subgrp*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:DatabaseClass rds:StorageSize rds:Piops	
RestoreDBClusterToPointInTime	Gewährt die Berechtigung zum Wiederherstellen eines DB-Clusters zu einem beliebigen Zeitpunkt	Write	cluster*		iam:PassRole rds:AddTagsToResource rds:CreateDBInstance
			cluster-pg*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			og*		
			subgrp*		
			cluster-auto-backup		
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:DatabaseClass rds:StorageSize rds:Piops	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RestoreDBInstanceFromDBSnapshot	Gewährt die Berechtigung zum Erstellen einer neuen DB-Instance aus einem DB-Snapshot	Write	db*		iam:PassRole rds:AddTagsToResource rds:CreateTenantDatabase
			og*		
			pg*		
			snapshot*		
			subgrp*		
				rds:BackupTarget aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RestoreDBInstanceFromS3	Gewährt die Berechtigung zum Erstellen einer neuen DB-Instance aus einem Amazon-S3-Bucket	Write	db*		iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey rds:AddTagsToResource secretsmanager:CreateSecret secretsmanager:TagResource
			og*		
			pg*		
			subgrp*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:ManageMasterUserPassword	
RestoreDBInstanceToPointInTime	Gewährt die Berechtigung zum Wiederherstellen einer DB-Instance zu einem beliebigen Zeitpunkt	Schreiben	db*		iam:PassRole rds:AddTagsToResource rds:CreateTenantDatabase
			og*		
			pg*		
			subgrp*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			auto-backup		
				rds:BackupTarget aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
RevokeDBSecurityGroupIngress	Erteilt die Erlaubnis, Zugriffe aus einer Datenbank SecurityGroup für zuvor autorisierte IP-Bereiche oder EC2- oder VPC-Sicherheitsgruppen zu widerrufen	Schreiben	secgrp*		
StartActivityStream	Gewährt die Berechtigung zum Starten von Aktivity Stream	Schreiben	cluster		
			db		
StartDBCluster	Gewährt die Berechtigung zum Starten des DB-Clusters	Schreiben	cluster*		
StartDBInstance	Gewährt die Berechtigung zum Starten der DB-Instance	Schreiben	db*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartDBInstanceAutomatedBackupsReplication	Erteilt die Berechtigung, die Replikation automatisierter Backups auf eine andere zu starten AWS-Region	Schreiben	auto-backup*		
			db*		
StartExportTask	Gewährt die Berechtigung zum Starten einer neuen Exportaufgabe für einen DB-Snapshot	Write			iam:PassRole
StopActivityStream	Gewährt die Berechtigung zum Beenden von Activity Stream	Write	cluster		
			db		
StopDBCluster	Gewährt die Berechtigung zum Beenden des DB-Clusters	Write	cluster*		
StopDBInstance	Gewährt die Berechtigung zum Beenden der DB-Instance	Write	db*		
StopDBInstanceAutomatedBackupsReplication	Gewährt die Berechtigung, die automatisierte Backup-Replikation für eine DB-Instance	Schreiben	db*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SwitchoverBlueGreenDeployment	Gewährt die Berechtigung zum Wechseln einer Blau/Grün-Bereitstellung von der Quell-Instance oder dem Cluster zur Ziel-Instance	Schreiben	deployment*		rds:ModifyDBCluster rds:ModifyDBInstance rds:PromoteReadReplica rds:PromoteReadReplicaDBCluster
				aws:ResourceTag/${TagKey}	
SwitchoverGlobalCluster	Gewährt die Berechtigung zum Umstellen eines globalen Clusters	Schreiben	cluster*		
			global-cluster*		
SwitchoverReadReplica	Erteilung der Berechtigung zum Umschalten einer Read Replica, wodurch diese zur neuen primären Datenbank wird	Schreiben	db*		

Von Amazon RDS definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
cluster	`arn:${Partition}:rds:${Region}:${Account}:cluster:${DbClusterInstanceName}`	aws:ResourceTag/${TagKey} rds:cluster-tag/${TagKey}
shardgrp	`arn:${Partition}:rds:${Region}:${Account}:shard-group:${DbShardGroupResourceId}`	
cluster-auto-backup	`arn:${Partition}:rds:${Region}:${Account}:cluster-auto-backup:${DbClusterAutomatedBackupId}`	
auto-backup	`arn:${Partition}:rds:${Region}:${Account}:auto-backup:${DbInstanceAutomatedBackupId}`	
cluster-endpoint	`arn:${Partition}:rds:${Region}:${Account}:cluster-endpoint:${DbClusterEndpoint}`	aws:ResourceTag/${TagKey}
cluster-pg	`arn:${Partition}:rds:${Region}:${Account}:cluster-pg:${ClusterParameterGroupName}`	aws:ResourceTag/${TagKey} rds:cluster-pg-tag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
cluster-snapshot	arn:${Partition}:rds:${Region}:${Account}:cluster-snapshot:${ClusterSnapshotName}	aws:ResourceTag/${TagKey} rds:cluster-snapshot-tag/${TagKey}
db	arn:${Partition}:rds:${Region}:${Account}:db:${DbInstanceName}	aws:ResourceTag/${TagKey} rds:DatabaseClass rds:DatabaseEngine rds:DatabaseName rds:MultiAz rds:Piops rds:StorageEncrypted rds:StorageSize rds:Vpc rds:db-tag/${TagKey}
es	arn:${Partition}:rds:${Region}:${Account}:es:${SubscriptionName}	aws:ResourceTag/${TagKey} rds:es-tag/${TagKey}
global-cluster	arn:${Partition}:rds::${Account}:global-cluster:${GlobalCluster}	

Ressourcentypen	ARN	Bedingungsschlüssel
og	arn:${Partition}:rds:${Region}:${Account}:og:${OptionGroupName}	aws:ResourceTag/${TagKey} rds:og-tag/${TagKey}
pg	arn:${Partition}:rds:${Region}:${Account}:pg:${ParameterGroupName}	aws:ResourceTag/${TagKey} rds:pg-tag/${TagKey}
proxy	arn:${Partition}:rds:${Region}:${Account}:db-proxy:${DbProxyId}	aws:ResourceTag/${TagKey}
proxy-endpoint	arn:${Partition}:rds:${Region}:${Account}:db-proxy-endpoint:${DbProxyEndpointId}	aws:ResourceTag/${TagKey}
ri	arn:${Partition}:rds:${Region}:${Account}:ri:${ReservedDbInstanceName}	aws:ResourceTag/${TagKey} rds:ri-tag/${TagKey}
secgrp	arn:${Partition}:rds:${Region}:${Account}:secgrp:${SecurityGroupName}	aws:ResourceTag/${TagKey} rds:secgrp-tag/${TagKey}
snapshot	arn:${Partition}:rds:${Region}:${Account}:snapshot:${SnapshotName}	aws:ResourceTag/${TagKey} rds:snapshot-tag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
subgrp	`arn:${Partition}:rds:${Region}:${Account}:subgrp:${SubnetGroupName}`	aws:ResourceTag/${TagKey} rds:subgrp-tag/${TagKey}
target-group	`arn:${Partition}:rds:${Region}:${Account}:target-group:${TargetGroupId}`	aws:ResourceTag/${TagKey}
cev	`arn:${Partition}:rds:${Region}:${Account}:cev:${Engine}/${EngineVersion}/${CustomDbEngineVersionId}`	aws:ResourceTag/${TagKey}
deployment	`arn:${Partition}:rds:${Region}:${Account}:deployment:${BlueGreenDeploymentIdentifier}`	aws:ResourceTag/${TagKey}
integration	`arn:${Partition}:rds:${Region}:${Account}:integration:${IntegrationIdentifier}`	aws:ResourceTag/${TagKey}
snapshot-tenant-database	`arn:${Partition}:rds:${Region}:${Account}:snapshot-tenant-database:${SnapshotName}:${TenantResourceId}`	aws:ResourceTag/${TagKey}
tenant-database	`arn:${Partition}:rds:${Region}:${Account}:tenant-database:${TenantResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon RDS

Amazon RDS definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Satz von Tag-Schlüssel-Wert-Paaren in der Anforderung	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert den Zugriff nach dem Satz von Tag-Schlüsseln in der Anforderung	ArrayOfString
rds:BackupTarget	Filtert den Zugriff nach dem Typ des Backup-Ziels. Einer von: REGION, OUTPOSTS	String
rds:CopyOptionGroup	Filtert den Zugriff nach dem Wert, der angibt, ob die DB-Optionsgruppe für die CopyDB-Optionsgruppe kopiert werden soll	Bool
rds:DatabaseClass	Filtert den Zugriff nach dem Typ der DB-Instance-Klasse	Zeichenfolge
rds:DatabaseEngine	Filtert den Zugriff nach dem Datenbank-Engine. Mögliche Werte finden Sie im Engine-Parameter in der CreateDBInstance-API	Zeichenfolge
rds:DatabaseName	Filtert den Zugriff nach benutzerdefiniertem Name der Datenbank auf der DB-Instance	Zeichenfolge
rds:EndpointType	Filtert den Zugriff nach dem Typ des Endpunkts. Einer der folgenden Typen: READER, WRITER, CUSTOM.	String
rds:ManageMasterUserPassword	Filtert den Zugriff nach dem Wert, der angibt, ob RDS das Master-Benutzerkennwort in AWS Secrets Manager für die DB-Instance oder den Cluster verwaltet.	Bool

Bedingungsschlüssel	Beschreibung	Typ
rds:MultiAz	Filtert den Zugriff nach dem Wert, der angibt, ob die DB-Instance in mehreren Availability Zones ausgeführt wird. Legen Sie „true“ fest, um anzugeben, dass die DB-Instance Multi-AZ verwendet	Bool
rds:MultiTenant	Filtert den Zugriff nach dem Wert, der angibt, ob sich die DB-Instance in der Multi-Tenant-Konfiguration befindet	String
rds:Piops	Filtert den Zugriff nach dem Wert, der die Anzahl der bereitgestellten IOPS (PIOPS) angibt, die von der Instance unterstützt werden. Legen Sie „0“ fest, um anzugeben, dass PIOPS für eine DB-Instance nicht aktiviert ist.	Numerischer Wert
rds:StorageEncrypted	Filtert den Zugriff nach dem Wert, der angibt, ob der DB-Instance-Speicher verschlüsselt werden soll. Um die Speicherverschlüsselung durchzusetzen, geben Sie „wahr“ an.	Bool
rds:StorageSize	Filtert den Zugriff nach der Größe des Speicher-Volumes (in GB)	Numerischer Wert
rds:TenantDatabaseName	Filtert den Zugriff nach dem Namen der Tenant-Datenbank in CreateTenantDatabase und nach dem Namen der neuen Tenant-Datenbank in ModifyTenantDatabase	String
rds:Vpc	Filtert den Zugriff nach dem Wert, der angibt, ob die DB-Instance in einer Amazon Virtual Private Cloud (Amazon VPC) ausgeführt wird. Weisen Sie „true“ zu, damit die DB-Instance in einer Amazon-VPC ausgeführt wird.	Bool
rds:cluster-pg-tag/${TagKey}	Filtert den Zugriff über das Tag, das einer DB-Cluster-Parametergruppe zugeordnet ist	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
rds:cluster-snapshot-tag/${TagKey}	Filtert den Zugriff über das Tag, das an einem DB-Cluster-Snapshot zugeordnet ist	Zeichenfolge
rds:cluster-tag/${TagKey}	Filtert den Zugriff über dass Tag, das einem DB-Cluster zugeordnet ist	Zeichenfolge
rds:db-tag/${TagKey}	Filtert den Zugriff über das Tag, das einer DB-Instance zugeordnet ist	Zeichenfolge
rds:es-tag/${TagKey}	Filtert den Zugriff über das Tag, das einem Ereignisabonnement zugeordnet ist	Zeichenfolge
rds:og-tag/${TagKey}	Filtert den Zugriff über das Tag, das einer DB-Optionsgruppe zugeordnet ist	Zeichenfolge
rds:pg-tag/${TagKey}	Filtert den Zugriff über das Tag, das einer DB-Parametergruppe zugeordnet ist	Zeichenfolge
rds:req-tag/${TagKey}	Filtert den Zugriff über die Gruppe von Tag-Schlüsseln und -Werten, die verwendet werden können, um eine Ressource zu kennzeichnen	Zeichenfolge
rds:ri-tag/${TagKey}	Filtert den Zugriff über das Tag, das einer reservierten DB-Instance zugeordnet ist	Zeichenfolge
rds:secgrp-tag/${TagKey}	Filtert den Zugriff über das Tag, das einer DB-Sicherheitsgruppe zugeordnet ist	Zeichenfolge
rds:snapshot-tag/${TagKey}	Filtert den Zugriff über das Tag, das einem DB-Snapshot zugeordnet ist	Zeichenfolge
rds:subgrp-tag/${TagKey}	Filtert den Zugriff nach dem Tag, das einer DB-Subnetzgruppe angefügt ist.	String

Aktionen, Ressourcen und Bedingungsschlüssel für die Amazon RDS-Daten-API

Amazon RDS-Daten-API (Servicepräfix: `rds-data`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von der Amazon RDS-Daten-API definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchExecuteStatement	Gewährt die Berechtigung zum Ausführen einer Batch-SQL-Anweisung über ein Array von Daten	Write	cluster*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
BeginTransaction	Gewährt die Berechtigung zum Starten einer SQL-Transaktion	Write	cluster*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
CommitTransaction	Gewährt die Berechtigung zum Beenden einer SQL-Transaktion, die mit der Produktion „BeginTransaction“ gestartet wurde, mit anschließender Übernahme der Änderungen	Write	cluster*		rds-data:BeginTransaction
				aws:ResourceTag/${TagKey} aws:TagKeys	
ExecuteSql	Gewährt die Berechtigung zum Ausführen einer oder mehrerer SQL-Anweisungen. Diese Produktion ist veraltet. Verwenden Sie die Produktion BatchExecuteStatement oder ExecuteStatement.	Write	cluster*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ExecuteStatement	Gewährt die Berechtigung zum Ausführen einer SQL-Anweisung für eine Datenbank	Write	cluster*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RollbackTransaction	Gewährt die Berechtigung zum Durchführen eines Rollbacks einer Transaktion. Durch das Rollback einer Transaktion werden zugehörige Änderungen rückgängig gemacht.	Write	cluster*		rds-data:BeginTransaction
				aws:ResourceTag/${TagKey} aws:TagKeys	

Von Amazon RDS Data API definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
cluster	`arn:${Partition}:rds:${Region}:${Account}:cluster:${DbClusterInstanceName}`	aws:ResourceTag/${TagKey} aws:TagKeys

Bedingungsschlüssel für die Amazon RDS-Daten-API

Die Amazon RDS-Daten-API definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie

verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach den Tag-Schlüsseln, die der Ressource zugeordnet sind	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für die Amazon RDS-IAM-Authentifizierung

Die Amazon RDS-IAM-Authentifizierung (Servicepräfix: `rds-db`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von der Amazon RDS-IAM-Authentifizierung definierte Aktionen
- Von Amazon RDS-IAM-Authentifizierung definierte Ressourcentypen
- Bedingungsschlüssel für die Amazon RDS-IAM-Authentifizierung

Von der Amazon RDS-IAM-Authentifizierung definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
connect	Ermöglicht einer IAM-Rolle oder einem IAM-Benutzer, eine Verbindung mit der RDS-Datenbank herzustellen	Berechtigungsverwaltung	db-user*		

Von Amazon RDS-IAM-Authentifizierung definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
db-user	`arn:${Partition}:rds-db:${Region}:${Account}:dbuser:${DbiResourceId}/${DbUserName}`	

Bedingungsschlüssel für die Amazon RDS-IAM-Authentifizierung

Die RDS-IAM-Authentifizierung umfasst keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS re:Post Private

AWS re:Post Private (Servicepräfix: `repostspace`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS re:POST Private definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSpace	Gewährt die Berechtigung zum Erstellen eines neuen privaten re:Post in Ihrem Konto	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteSpace	Gewährt die Berechtigung zum Löschen eines privaten re:Post aus dem Konto.	Schreiben	space*		
DeregisterAdmin	Gewährt die Berechtigung, einen Administrator von einem	Schreiben	space*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	privaten re:Post in deinem Konto zu entfernen				
GetSpace	Gewährt die Berechtigung zum Abrufen einer Beschreibung eines privaten re:Post in deinem Konto	Lesen	space*		
ListSpaces	Gewährt die Berechtigung zum Auflisten aller privaten re:Post in Ihrem Konto	Lesen			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags, die einer Ressource zugeordnet sind	Lesen	space*		
				aws:TagKeys aws:RequestTag/${TagKey}	
RegisterAdmin	Gewährt die Berechtigung, einem privaten re:post in Ihrem Konto einen Administrator hinzuzufügen	Schreiben	space*		
SendInvites	Gewährt die Berechtigung, Einladungen an Nutzer eines privaten re:Posts in Ihrem Konto zu senden	Schreiben	space*		
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren	space*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Markierung	space*		
				aws:TagKeys	
UpdateSpace	Gewährt die Berechtigung zum Aktualisieren einer Tabelle in Ihrem Konto	Schreiben	space*		

Von AWS re:Post Private definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
space	`arn:${Partition}:repostspace:${Region}:${Account}:space/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS re:Post Private

AWS re:Post Private definiert die folgenden Bedingungsschlüssel, die in einem `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Recycle Bin

AWS-Papierkorb (Servicepräfix: `rbin`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Recycle Bin definierte Aktionen

- Von AWS Recycle Bin definierte Ressourcentypen
- Bedingungsschlüssel für AWS Recycle Bin

Von AWS Recycle Bin definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateRule	Gewährt die Berechtigung zum Erstellen einer Recycle-Bin-Aufbewahrungsregel	Schreiben	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys rbin:Request/ResourceType	
DeleteRule	Gewährt die Berechtigung zum Löschen einer Recycle-Bin-Aufbewahrungsregel	Schreiben	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
GetRule	Gewährt die Berechtigung zum Abrufen detaillierter Informationen zu einer Recycle-Bin-Aufbewahrungsregel	Lesen	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/Res	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ourceType	
ListRules	Gewährt die Berechtigung zum Auflisten der Recycle-Bin-Aufbewahrungsregeln in der Region	Lesen		rbin:Request/ResourceType	
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags, die einer Ressource zugeordnet sind	Lesen	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
LockRule	Gewährt die Berechtigung zum Sperren einer Papierkorb-Aufbewahrungsregel	Schreiben	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
TagResource	Gewährt die Berechtigung zum Hinzufügen oder Aktualisieren von Tags einer Ressource	Markierung	rule*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys rbin:Attribute/ResourceType	
UnlockRule	Gewährt die Berechtigung zum Entsperren einer Papierkorb-Aufbewahrungsregel	Schreiben	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags, die einer Ressource zugeordnet sind.	Markierung	rule*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} aws:TagKeys rbin:Attribute/ResourceType	
UpdateRule	Gewährt die Berechtigung zum Aktualisieren einer Recycle-Bin-Aufbewahrungsregel	Schreiben	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	

Von AWS Recycle Bin definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
rule	`arn:${Partition}:rbin:${Region}:${Account}:rule/${ResourceName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Recycle Bin

AWS Recycle Bin definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Schlüssel eines Tags und den Wert einer Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach den Tag-Schlüsseln in einer Anforderung	ArrayOfString
rbin:Attribute/ResourceType	Filtert den Zugriff nach dem Ressourcen-Typ der bestehenden Regel	Zeichenfolge
rbin:Request/ResourceType	Filtert den Zugriff nach dem Ressourcen-Typ in einer Anforderung	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Redshift

Amazon Redshift (Servicepräfix: `redshift`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Redshift definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWSzu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptReservedNodeExchange	Gewährt die Berechtigung zum Austausch eines reservierten DC1-Knotens gegen einen reservierten DC2-Knoten ohne Änderungen an der Konfiguration	Schreiben			
AddPartner	Gewährt die Berechtigung zum Hinzufügen einer Partnerintegration zu einem Cluster	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateDataShareConsumer	Gewährt die Berechtigung, einen Verbraucher einem Datashare zu zuordnen	Write	datashare*		
				redshift:ConsumerArn redshift:AllowWrites	
AuthorizeClusterSecurityGroupIngress	Gewährt die Berechtigung, einer Amazon Redshift-Sicherheitsgruppe eine eingehende Regel hinzuzufügen	Schreiben	securitygroup*		
			securitygroupingress-ec2securitygroup*		
AuthorizeDataShare	Gewährt die Berechtigung, dem angegebenen Datashare Consumer die Verwendung eines Datenspeichers zu autorisieren	Berechtigungsverwaltung	datashare*		
				redshift:ConsumerIdentifier redshift:AllowWrites	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AuthorizeEndpointAccess	Gewährt die Berechtigung zum Autorisieren von endpunktbezogenen Aktivitäten für von Redshift verwaltete VPC-Endpunkte	Berechtigungsverwaltung			
AuthorizeSnapshotAccess	Gewährt dem angegebenen die Berechtigung AWS-Konto zum Wiederherstellen eines Snapshots	Berechtigungsverwaltung	snapshot*		
BatchDeleteClusterSnapshots	Gewährt die Berechtigung zum Löschen von Snapshots in einem Batch mit einer Größe von bis zu 100	Write	snapshot*		
BatchModifyClusterSnapshots	Gewährt die Berechtigung zum Ändern von Einstellungen für eine Snapshot-Liste	Write	snapshot*		
CancelQuery [nur Berechtigung]	Gewährt die Berechtigung zum Abbrechen einer Abfrage über die Amazon Redshift-Konsole	Write			
CancelQuerySession [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen von Abfragen in der Amazon Redshift-Konsole	Write			
CancelResize	Gewährt die Berechtigung zum Abbrechen einer GrößenänderungsProduktion	Write	cluster*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CopyClusterSnapshot	Gewährt die Berechtigung zum Kopieren eines Cluster-Snapshots	Schreiben	snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAuthenticationProfile	Gewährt die Berechtigung zum Erstellen eines Amazon-Redshift-Authentifizierungsprofils	Schreiben			
CreateCluster	Gewährt die Berechtigung zum Erstellen eines Clusters	Write	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterParameterGroup	Gewährt die Berechtigung zum Erstellen einer Amazon Redshift-Parametergruppe	Write	parametergroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateClusterSecurityGroup	Gewährt die Berechtigung zum Erstellen einer Amazon Redshift-Sicherheitsgruppe	Write	securitygroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterSnapshot	Gewährt die Berechtigung, einen manuellen Snapshot des angegebenen Clusters zu erstellen	Write	snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterSubnetGroup	Gewährt die Berechtigung zum Erstellen einer Amazon Redshift-Subnetzgruppe	Write	subnetgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterUser	Gewährt die Berechtigung, den angegebenen Amazon Redshift-Benutzer automatisch zu erstellen, wenn er nicht existiert	Berechtigungsverwaltung	dbuser*		
				redshift:DbUser	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCustomDomainAssociation	Gewährt die Berechtigung zum Erstellen eines benutzerdefinierten Domain-Namens für einen Cluster	Schreiben	cluster*		acm:DescribeCertificate
CreateEndpointAccess	Gewährt die Berechtigung zum Erstellen eines von Redshift verwalteten VPC-Endpunkts	Schreiben			
CreateEventSubscription	Gewährt die Berechtigung zum Erstellen eines Amazon Redshift-Ereignisbenachrichtigungsabonnements	Write	eventsubscription*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHsmClientCertificate	Gewährt die Berechtigung zum Erstellen eines HSM-Client-Zertifikats, das ein Cluster verwendet, um eine Verbindung zu einem HSM herzustellen	Write	hsmclientcertificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateHsmConfiguration	Gewährt die Berechtigung zum Erstellen einer HSM-Konfiguration, die die von einem Cluster zum Speichern und Verwenden von Datenbank-Verschlüsselungsschlüsseln in einem Hardwaresicherheitsmodul (HSM) benötigten Informationen enthält	Write	hsmconfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateQev2IdcApplication [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer Qev2-IDC-Anwendung	Schreiben			sso:CreateApplication sso:PutApplicationAccessScope sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateRedshiftIdcApplication	Gewährt die Berechtigung zum Erstellen einer Redshift-IDC-Anwendung	Schreiben			sso:CreateApplication sso:PutApplicationAccessScope sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant
CreateSavedQuery [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen gespeicherter SQL-Abfragen über die Amazon Redshift-Konsole	Write			
CreateScheduledAction	Gewährt die Berechtigung zum Erstellen einer geplanten Amazon Redshift-Aktion	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSnapshotCopyGrant	Gewährt die Berechtigung zum Erstellen einer Snapshot-Kopierberechtigung und zum Verschlüsseln kopierter Snapshots in einem Ziel AWS-Region	Berechtigungsverwaltung	snapshotcopygrant*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshotSchedule	Gewährt die Berechtigung zum Erstellen eines Snapshot-Zeitplans	Write	snapshotschedule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTags	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Tags zu einer bestimmten Ressource	Markieren	cluster		
			dbgroup		
			dbname		
			dbuser		
			eventsubscription		
			hsmclientcertificate		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			hsmconfiguration		
			parametergroup		
			securitygroup		
			securitygroupingress-cidr		
			securitygroupingress-ec2securitygroup		
			snapshot		
			snapshotcopygrant		
			snapshotschedule		
			subnetgroup		
			usagelimit		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUsageLimit	Gewährt die Berechtigung zum Erstellen eines Nutzungslimits	Schreiben	usagelimit*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeauthorizeDataShare	gewährt die Berechtigung zum Entfernen der Berechtigung aus dem angegebenen Datashare Consumer zum Verbrauchen eines Datenaustauschs	Berechtigungsverwaltung	datashare*		
				redshift:ConsumerIdentifier	
DeleteAuthenticationProfile	Gewährt die Berechtigung zum Löschen eines Amazon-Redshift-Authentifizierungsprofils	Schreiben			
DeleteCluster	Gewährt die Berechtigung zum Löschen eines zuvor bereitgestellten Clusters	Write	cluster*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteClusterParameterGroup	Gewährt die Berechtigung zum Löschen einer Amazon Redshift-Parametergruppe	Write	parametergroup*		
DeleteClusterSecurityGroup	Gewährt die Berechtigung zum Löschen einer Amazon Redshift-Sicherheitsgruppe	Write	securitygroup*		
DeleteClusterSnapshot	Gewährt die Berechtigung zum Löschen eines manuellen Snapshots	Write	snapshot*		
DeleteClusterSubnetGroup	Gewährt die Berechtigung zum Löschen einer Cluster-Subnetzgruppe	Schreiben	subnetgroup*		
DeleteCustomDomainAssociation	Gewährt die Berechtigung zum Löschen eines benutzerdefinierten Domain-Namens für einen Cluster	Schreiben	cluster*		
DeleteEndpointAccess	Gewährt die Berechtigung zum Löschen eines von Redshift verwalteten VPC-Endpunkts	Schreiben			
DeleteEventSubscription	Gewährt die Berechtigung zum Löschen eines Amazon Redshift-Ereignisbenachrichtigungsabonnements	Write	eventsubscription*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteHsmClientCertificate	Gewährt die Berechtigung zum Löschen eines HSM-Client-Zertifikats	Write	hsmclientcertificate*		
DeleteHsmConfiguration	Gewährt die Berechtigung zum Löschen einer Amazon Redshift HSM-Konfiguration	Schreiben	hsmconfiguration*		
DeletePartner	Gewährt die Berechtigung zum Löschen einer Partnerintegration aus einem Cluster	Schreiben			
DeleteQev2IdcApplication [nur Berechtigung]	Gewährt die Berechtigung zum Löschen einer Qev2-IDC-Anwendung	Schreiben	qev2idcapplication*		sso:DeleteApplication
DeleteRedshiftIdcApplication	Gewährt die Berechtigung zum Löschen einer Redshift-IDC-Anwendung	Schreiben	redshiftidcapplication*		sso:DeleteApplication
DeleteResourcePolicy	Gewährt die Berechtigung zum Löschen der ressourcenbasierten Richtlinie einer angegebenen Ressource	Berechtigungsverwaltung	namespace*		
DeleteSavedQueries [nur Berechtigung]	Gewährt die Berechtigung zum Löschen gespeicherter SQL-Abfragen über die Amazon Redshift-Konsole	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteScheduledAction	Gewährt die Berechtigung zum Löschen einer geplanten Amazon Redshift-Aktion	Write			
DeleteSnapshotCopyGrant	Gewährt die Berechtigung zum Löschen einer Snapshot-Kopier-Berechtigung	Write	snapshotcopygrant*		
DeleteSnapshotSchedule	Gewährt die Berechtigung zum Löschen eines Snapshot-Zeitplans	Write	snapshotschedule*		
DeleteTags	Gewährt die Berechtigung zum Löschen eines oder mehrerer Tags aus einer Ressource	Markieren	cluster		
			dbgroup		
			dbname		
			dbuser		
			eventsubscription		
			hsmclientcertificate		
			hsmconfiguration		
			parametergroup		
			securitygroup		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			securitygroupingress-cidr		
			securitygroupingress-ec2securitygroup		
			snapshot		
			snapshotcopygrant		
			snapshotschedule		
			subnetgroup		
			usagelimit		
				aws:TagKeys	
DeleteUsageLimit	Gewährt die Berechtigung zum Löschen eines Nutzungslimits	Schreiben	usagelimit*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeAccountAttributes	Gewährt die Berechtigung zum Beschreiben von Attributen, die an das angegebene angefügt sind AWS-Konto	Lesen			
DescribeAuthenticationProfiles	Gewährt die Berechtigung zum Beschreiben eines Amazon-Redshift-Authentifizierungsprofils	Lesen			
DescribeClusterDbRevisions	Gewährt die Berechtigung zum Beschreiben von Datenbankrevisionen für einen Cluster	List			
DescribeClusterParameterGroups	Gewährt die Berechtigung zum Beschreiben einer Liste der Amazon Redshift-Parametergruppen, einschließlich der von Ihnen erstellten Parametergruppen und der Standardparametergruppe	Read			
DescribeClusterParameters	Gewährt die Berechtigung zum Beschreiben von Parametern, die in einer Amazon Redshift-Parametergruppe enthalten sind	Read	parametergroup*		
DescribeClusterSecurityGroups	Gewährt die Berechtigung zum Beschreiben von Amazon Redshift-Sicherheitsgruppen	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeClusterSnapshots	Gewährt die Berechtigung zum Beschreiben eines oder mehrerer Snapshot-Objekte, die Metadaten zu den Cluster-Snapshots enthalten	Read			
DescribeClusterSubnetGroups	Gewährt die Berechtigung zum Beschreiben mindestens eines Cluster-Subnetzgruppenobjekts, das Metadaten zu Cluster-Subnetzgruppen enthält	Read			
DescribeClusterTracks	Gewährt die Berechtigung zum Beschreiben verfügbarer Wartungsspuren	List			
DescribeClusterVersions	Gewährt die Berechtigung zur Beschreibung der verfügbaren Amazon Redshift-Cluster-Versionen	Read			
DescribeClusters	Gewährt die Berechtigung zum Beschreiben von Eigenschaften bereitgestellter Cluster	Auflisten			
DescribeCustomDomainAssociations	Gewährt die Berechtigung zum Beschreiben eines benutzerdefinierten Domain-Namens für einen Cluster	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDataShares	Gewährt die Berechtigung zum Beschreiben von Datashares, die von Ihren Clustern erstellt und verwendet werden	Read			
DescribeDataSharesForConsumer	Gewährt die Berechtigung, nur Datashares zu beschreiben, die von Ihren Clustern verwendet werden	Read			
DescribeDataSharesForProducer	Gewährt die Berechtigung, nur Datashares zu beschreiben, die von Ihren Clustern erstellt wurden	Read			
DescribeDefaultClusterParameters	Gewährt die Berechtigung zum Beschreiben von Parametereinstellungen für eine Parametergruppenfamilie	Lesen			
DescribeEndpointAccess	Gewährt die Berechtigung, von Redshift verwaltete VPC-Endpunkte zu beschreiben	Lesen			
DescribeEndpointAuthorization	Gewährt die Berechtigung, die Beschreibungsaktivität für von Redshift verwaltete VPC-Endpunkte zu autorisieren	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeEventCategories	Gewährt die Berechtigung zum Beschreiben von Ereigniskategorien für alle Ereignisquelltypen oder für einen angegebenen Quelltyp	Lesen			
DescribeEventSubscriptions	Gewährt die Berechtigung zum Beschreiben von Abonnements für Amazon-Redshift-Ereignisbenachrichtigungen für das angegebene AWS-Konto	Lesen			
DescribeEvents	Gewährt die Berechtigung zum Beschreiben der Ereignisse bezüglich Clustern, Sicherheitsgruppen, Snapshots und Parametergruppen in den vergangenen 14 Tagen	List			
DescribeHsmClientCertificates	Gewährt die Berechtigung zum Beschreiben von HSM-Client-Zertifikaten	Read			
DescribeHsmConfigurations	Gewährt die Berechtigung zum Beschreiben von Amazon Redshift HSM-Konfigurationen	Lesen			
DescribeInboundIntegrations	Gewährt die Berechtigung zum Auflisten der eingehenden Integrationen	Auflisten		redshift:InboundIntegrationArn	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeLoggingStatus	Gewährt die Berechtigung zu beschreiben, ob Informationen wie Abfragen und Verbindungsversuche für einen Cluster protokolliert werden	Read	cluster*		
DescribeNodeConfigurationOptions	Gewährt die Berechtigung zum Beschreiben von Eigenschaften möglicher Knotenkonfigurationen wie Knotentyp, Anzahl der Knoten und Festplattenbelegung für den angegebenen Aktionstyp	List			
DescribeOrderableClusterOptions	Gewährt die Berechtigung zum Beschreiben von sortierbaren Cluster-Optionen	Lesen			
DescribePartners	Gewährt die Berechtigung zum Abrufen von Informationen zu den für einen Cluster definierten Partnerintegrationen	Lesen			
DescribeQev2IdcApplications [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben von Qev2-IDC-Anwendungen	Auflisten			
DescribeQuery [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben einer Abfrage über die Amazon Redshift-Konsole	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeRedshiftIdcApplications	Gewährt die Berechtigung zum Beschreiben von Redshift-IDC-Anwendungen	Auflisten			sso:GetApplicationGrant sso:ListApplicationAccessScopes
DescribeReservedNodeExchangeStatus	Erteilt die Berechtigung, Austauschstatusdetails und zugehörige Metadaten für einen Austausch mit reservierten Knoten zu beschreiben. Zu den Status gehören Werte wie „in Bearbeitung“ und „Angefordert“	Lesen			
DescribeReservedNodeOfferings	Gewährt die Berechtigung zum Beschreiben verfügbarer reservierter Knotenangebote durch Amazon Redshift	Read			
DescribeReservedNodes	Gewährt die Berechtigung zum Beschreiben der reservierten Knoten	Read			
DescribeResize	Gewährt die Berechtigung zum Beschreiben der letzten GrößenänderungsProduktion für einen Cluster	Read	cluster*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeSavedQueries [nur Berechtigung]	Gewährt die Berechtigung, gespeicherte Abfragen über die Amazon Redshift-Konsole zu beschreiben	Read			
DescribeScheduledActions	Gewährt die Berechtigung zum Beschreiben von erstellten und geplanten Amazon Redshift-Aktionen	Lesen			
DescribeSnapshotCopyGrants	Gewährt die Berechtigung zum Beschreiben von Snapshot-Kopierberechtigungen, die dem AWS-Konto im Ziel angegebenen gehören AWS-Region	Lesen			
DescribeSnapshotSchedules	Gewährt die Berechtigung zum Beschreiben von Snapshot-Zeitplänen	Read	snapshotschedule*		
DescribeStorage	Gewährt die Berechtigung zum Beschreiben der Sicherungsspeichergröße und des vorläufigen Speichers auf Kontoebene	Read			
DescribeTable [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben einer Tabelle über die Amazon Redshift-Konsole	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeTableRestoreStatus	Gewährt die Berechtigung zum Beschreiben des Status einer oder mehrerer Tabellenwiederherstellungsanforderungen, die mit der RestoreTableFromClusterSnapshot -API-Aktion gestellt wurden	Lesen			
DescribeTags	Gewährt die Berechtigung, Tags zu beschreiben	Read	cluster		
			dbgroup		
			dbname		
			dbuser		
			eventsubscription		
			hsmclientcertificate		
			hsmconfiguration		
			parametergroup		
			securitygroup		
			securitygroupingress-cidr		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			securitygroupingress-ec2securitygroup		
			snapshot		
			snapshotcopygrant		
			snapshotschedule		
			subnetgroup		
			usagelimit		
DescribeUsageLimits	Gewährt die Berechtigung zum Beschreiben von Nutzungslimits	Read	usagelimit*		
DisableLogging	Gewährt die Berechtigung zum Deaktivieren von Protokollierungsinformationen, z. B. Abfragen und Verbindungsversuche, für einen Cluster	Write	cluster*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisableSnapshotCopy	Gewährt die Berechtigung zum Deaktivieren der automatischen Kopie von Snapshots für einen Cluster	Write	cluster*		
DisassociateDataShareConsumer	Gewährt die Berechtigung, einen Verbraucher von einem Datashare zu trennen	Write	datashare*		
				redshift:ConsumerArn	
EnableLogging	Gewährt die Berechtigung zum Aktivieren von Protokollierungsinformationen, z. B. Abfragen und Verbindungsversuche, für einen Cluster	Write	cluster*		
EnableSnapshotCopy	Gewährt die Berechtigung zum Aktivieren der automatischen Kopie von Snapshots für einen Cluster	Write	cluster*		
ExecuteQuery [nur Berechtigung]	Gewährt die Berechtigung zum Ausführen einer Abfrage über die Amazon Redshift-Konsole	Schreiben			
FailoverPrimaryCompute	Gewährt die Berechtigung zum Failover der primären Datenverarbeitung eines Multi-AZ-Clusters auf eine andere AZ	Schreiben	cluster*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
FetchResults [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Abfrageergebnissen über die Amazon Redshift-Konsole	Lesen			
GetClusterCredentials	Gewährt die Berechtigung zum Abrufen temporärer Anmeldeinformationen für den Zugriff auf eine Amazon-Redshift-Datenbank durch das angegebene AWS-Konto	Schreiben	dbuser*		
			dbgroup		
			dbname		
				redshift:DbName redshift:DbUser redshift:DurationSeconds	
GetClusterCredentialsWithIAM	Gewährt die Berechtigung zum Abrufen erweiterter temporärer Anmeldeinformationen für den Zugriff auf eine Amazon-Redshift-Datenbank durch das angegebene AWS-Konto	Schreiben	dbname		
				redshift:DbName redshift:DurationSeconds	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetReservedNodeExchangeConfigurationOptions	Gewährt die Berechtigung zum Abrufen von Konfigurationsoptionen für den Austausch mit reserviertem Knoten	Lesen			
GetReservedNodeExchangeOfferings	Gewährt die Berechtigung zum Abrufen eines Arrays von DC2 ReservedNodeOfferings , das dem Zahlungstyp, der Laufzeit und dem Nutzungspreis des angegebenen reservierten DC1-Knotens entspricht	Lesen			
GetResourcePolicy	Gewährt die Berechtigung zum Abrufen der ressourcenbasierten Richtlinie für die angegebene Ressource	Lesen	namespace*		
JoinGroup	Gewährt die Berechtigung, der angegebenen Amazon Redshift-Gruppe beizutreten	Berechtigungsverwaltung	dbgroup*		
ListDatabases [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Datenbanken über die Amazon Redshift-Konsole	Auflisten			
ListRecommendations	Gewährt die Berechtigung zum Auflisten von Advisor-Empfehlungen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListSavedQueries [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten gespeicherter Abfragen über die Amazon Redshift-Konsole	List			
ListSchemas [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Schemata über die Amazon Redshift-Konsole	List			
ListTables [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Tabellen über die Amazon Redshift-Konsole	List			
ModifyAquaConfiguration	Gewährt die Erlaubnis, die AQUA-Konfiguration eines Clusters zu ändern	Schreiben	cluster*		
ModifyAuthenticationProfile	Gewährt die Berechtigung zum Ändern eines Amazon-Redshift-Authentifizierungsprofils	Schreiben			
ModifyCluster	Gewährt die Berechtigung zum Ändern der Einstellungen eines Clusters	Write	cluster*		acm:DescribeCertificate
ModifyClusterDbRevision	Gewährt die Berechtigung zum Ändern der Datenbankversion eines Clusters	Schreiben	cluster*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyClusterIamRoles	Gewährt die Berechtigung zum Ändern der Liste der AWS Identity and Access Management (IAM)-Rollen, die von einem Cluster für den Zugriff auf andere - AWS Services verwendet werden können	Berechtigungsverwaltung	cluster*		
ModifyClusterMaintenance	Gewährt die Berechtigung zum Ändern der Wartungseinstellungen eines Clusters	Write			
ModifyClusterParameterGroup	Gewährt die Berechtigung zum Ändern der Parameter einer Parametergruppe	Write	parametergroup*		
ModifyClusterSnapshot	Gewährt die Berechtigung zum Ändern der Einstellungen eines Snapshots	Write	snapshot*		
ModifyClusterSnapshotSchedule	Gewährt die Berechtigung zum Ändern des Snapshot-Zeitplans für einen Cluster	Write	cluster*		
ModifyClusterSubnetGroup	Gewährt die Berechtigung, eine Cluster-Subnetzgruppe so zu ändern, dass sie die angegebene Liste der VPC-Subnetze enthält	Schreiben	subnetgroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyCustomDomainAssociation	Gewährt die Berechtigung zum Ändern eines benutzerdefinierten Domain-Namens für einen Cluster	Schreiben	cluster*		acm:DescribeCertificate
ModifyEndpointAccess	Gewährt die Berechtigung zum Ändern eines von Redshift verwalteten VPC-Endpunkts	Schreiben			
ModifyEventSubscription	Gewährt die Berechtigung zum Ändern eines bestehenden Amazon Redshift-Ereignisbenachrichtigungsabonnements	Write	eventsubscription*		
ModifyQev2IdcApplication [nur Berechtigung]	Gewährt die Berechtigung zum Ändern einer Qev2-IDC-Anwendung	Schreiben	qev2idcapplication*		sso:UpdateApplication

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyRedshiftIdcApplication	Gewährt die Berechtigung zum Ändern einer Redshift-IDC-Anwendung	Schreiben	redshiftidcapplication*		sso:DeleteApplicationAccessScope sso:DeleteApplicationGrant sso:GetApplicationGrant sso:ListApplicationAccessScopes sso:PutApplicationAccessScope sso:PutApplicationGrant sso:UpdateApplication

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifySavedQuery [nur Berechtigung]	Gewährt die Berechtigung, eine vorhandene gespeicherte Abfrage über die Amazon Redshift-Konsole zu ändern	Write			
ModifyScheduledAction	Gewährt die Berechtigung zum Ändern einer bestehenden geplanten Amazon Redshift-Aktion	Schreiben			
ModifySnapshotCopyRetentionPeriod	Gewährt die Berechtigung zum Ändern der Anzahl der Tage, wie lange Snapshots im Ziel aufbewahrt werden sollen, AWS-Region nachdem sie aus der Quelle kopiert wurden AWS-Region	Schreiben	cluster*		
ModifySnapshotSchedule	Gewährt die Berechtigung zum Ändern eines Snapshot-Zeitplans	Write	snapshotschedule*		
ModifyUsageLimit	Gewährt die Berechtigung zum Ändern eines Nutzungslimits	Write	usagelimit*		
PauseCluster	Gewährt die Berechtigung zum Anhalten eines Clusters	Write	cluster*		
PurchaseReservedNodeOffering	Gewährt die Berechtigung zum Kauf eines reservierten Knotens	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutResourcePolicy	Gewährt die Berechtigung zum Aktualisieren einer ressourcenbasierten Richtlinie für die angegebene Ressource	Berechtigungsverwaltung	namespace*		
RebootCluster	Gewährt die Berechtigung, einen Cluster neu zu starten	Write	cluster*		
RejectDataShare	Gewährt die Berechtigung zum Ablehnen eines Datashare, der von einem anderen Konto	Permissions management	datashare*		
ResetClusterParameterGroup	Gewährt die Berechtigung zum Festlegen einzelner oder mehrerer Parameter der angegebenen Parametergruppe auf die Standardwerte und zum Zuweisen als Ausgangswert für die Parameter „engine-default“	Write	parametergroup*		
ResizeCluster	Gewährt die Berechtigung, die Größe eines Clusters zu ändern	Write	cluster*		
RestoreFromClusterSnapshot	Gewährt die Berechtigung zum Erstellen eines Clusters aus einem Snapshot	Write	cluster*		
			snapshot*		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RestoreTableFromClusterSnapshot	Gewährt die Berechtigung, aus einer Tabelle in einem Amazon Redshift-Cluster-Snapshot eine Tabelle zu erstellen	Write	cluster*		
			snapshot*		
ResumeCluster	Gewährt die Berechtigung, die Ausführung eines Cluster fortzusetzen	Write	cluster*		
RevokeClusterSecurityGroupIngress	Gewährt die Berechtigung zum Widerrufen einer Regel für eingehenden Datenverkehr in einer Amazon Redshift-Sicherheitsgruppe für einen zuvor autorisierten IP-Bereich oder eine Amazon EC2-Sicherheitsgruppe	Schreiben	securitygroup*		
			securitygroupingress-ec2securitygroup*		
RevokeEndpointAccess	Gewährt die Berechtigung zum Aufheben des Zugriffs für endpunktbezogene Aktivitäten für von Redshift verwaltete VPC-Endpunkte	Berechtigungsverwaltung			
RevokeSnapshotAccess	Gewährt die Berechtigung zum Widerrufen des Zugriffs auf das angegebene AWS-Konto , um einen Snapshot wiederherzustellen	Berechtigungsverwaltung	snapshot*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RotateEncryptionKey	Gewährt die Berechtigung zum Rotieren des Verschlüsselungsschlüssels für einen Cluster	Schreiben	cluster*		
UpdatePartnerStatus	Gewährt die Berechtigung zum Aktualisieren des Status einer Partnerintegration	Schreiben			
ViewQueriesFromConsole [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen von Abfrageergebnissen über die Amazon Redshift-Konsole	List			
ViewQueriesInConsole [nur Berechtigung]	Gewährt die Berechtigung zum Beenden von Abfragen und Lasten über die Amazon Redshift-Konsole	List			

Von Amazon Redshift definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
cluster	arn:${Partition}:redshift:${Region}:${Account}:cluster:${ClusterName}	aws:ResourceTag/${TagKey}
datashare	arn:${Partition}:redshift:${Region}:${Account}:datashare:${ProducerClusterNamespace}/${DataShareName}	aws:ResourceTag/${TagKey}
dbgroup	arn:${Partition}:redshift:${Region}:${Account}:dbgroup:${ClusterName}/${DbGroup}	aws:ResourceTag/${TagKey}
dbname	arn:${Partition}:redshift:${Region}:${Account}:dbname:${ClusterName}/${DbName}	aws:ResourceTag/${TagKey}
dbuser	arn:${Partition}:redshift:${Region}:${Account}:dbuser:${ClusterName}/${DbUser}	aws:ResourceTag/${TagKey}
eventsubscription	arn:${Partition}:redshift:${Region}:${Account}:eventsubscription:${EventSubscriptionName}	aws:ResourceTag/${TagKey}
hsmclientcertificate	arn:${Partition}:redshift:${Region}:${Account}:hsmclientcertificate:${HSMClientCertificateId}	aws:ResourceTag/${TagKey}
hsmconfiguration	arn:${Partition}:redshift:${Region}:${Account}:hsmconfiguration:${HSMConfigurationId}	aws:ResourceTag/${TagKey}
namespace	arn:${Partition}:redshift:${Region}:${Account}:namespace:${ClusterNamespace}	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
parametergroup	arn:${Partition}:redshift:${Region}:${Account}:parametergroup:${ParameterGroupName}	aws:ResourceTag/${TagKey}
securitygroup	arn:${Partition}:redshift:${Region}:${Account}:securitygroup:${SecurityGroupName}/ec2securitygroup/${Owner}/${Ec2SecurityGroupId}	aws:ResourceTag/${TagKey}
securitygroupingress-cidr	arn:${Partition}:redshift:${Region}:${Account}:securitygroupingress:${SecurityGroupName}/cidrip/${IpRange}	aws:ResourceTag/${TagKey}
securitygroupingress-ec2securitygroup	arn:${Partition}:redshift:${Region}:${Account}:securitygroupingress:${SecurityGroupName}/ec2securitygroup/${Owner}/${Ece2SecuritygroupId}	aws:ResourceTag/${TagKey}
snapshot	arn:${Partition}:redshift:${Region}:${Account}:snapshot:${ClusterName}/${SnapshotName}	aws:ResourceTag/${TagKey}
snapshotcopygrant	arn:${Partition}:redshift:${Region}:${Account}:snapshotcopygrant:${SnapshotCopyGrantName}	aws:ResourceTag/${TagKey}
snapshotschedule	arn:${Partition}:redshift:${Region}:${Account}:snapshotschedule:${ParameterGroupName}	aws:ResourceTag/${TagKey}
subnetgroup	arn:${Partition}:redshift:${Region}:${Account}:subnetgroup:${SubnetGroupName}	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
usagelimit	`arn:${Partition}:redshift:${Region}:${Account}:usagelimit:${UsageLimitId}`	aws:ResourceTag/${TagKey}
redshiftidcapplication	`arn:${Partition}:redshift:${Region}:${Account}:redshiftidcapplication:${RedshiftIdcApplicationId}`	
qev2idcapplication	`arn:${Partition}:redshift:${Region}:${Account}:qev2idcapplication:${Qev2IdcApplicationId}`	

Bedingungsschlüssel für Amazon Redshift

Amazon Redshift definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Zugriff nach Aktionen, basierend auf den zulässigen Werten für die einzelnen Tags	String
aws:ResourceTag/${TagKey}	Filtert Zugriff nach Aktionen, basierend auf dem Tag-Wert, der der Ressource zugeordnet ist	String
aws:TagKeys	Filtert Zugriff nach Aktionen, basierend auf den obligatorischen Tags in der Anforderung	ArrayOfString

Bedingungsschlüssel	Beschreibung	Typ
redshift:AllowWrites	Filtert den Zugriff nach dem Eingabeparameter AllowWrites	Bool
redshift:ConsumerArn	Filtert den Zugriff nach Datashare-Consumer-ARN.	ARN
redshift:ConsumerIdentifier	Filtert den Zugriff nach Datashare Consumer	Zeichenfolge
redshift:DbName	Filtert den Zugriff nach dem Datenbanknamen	Zeichenfolge
redshift:DbUser	Filtert den Zugriff nach dem Datenbankbenutzernamen	Zeichenfolge
redshift:DurationSeconds	Filtern Zugriff nach der Anzahl der Sekunden bis zum Ablauf eines Satzes temporärer Anmeldeinformationen	String
redshift:InboundIntegrationArn	Filtert den Zugriff nach dem ARN einer eingehenden Null-ETL-Integrationsressource	String

Aktionen, Ressourcen und Bedingungsschlüssel für die Amazon Redshift-Daten-API

Die Amazon Redshift-Daten-API (Servicepräfix: `redshift-data`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von der Amazon Redshift-Daten-API definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchExecuteStatement	Gewährt die Berechtigung zum Ausführen mehrerer Abfragen unter einer einzigen Verbindung	Schreiben	cluster*		
			workgroup* –		
CancelStatement	Gewährt die Berechtigung zum Abbrechen einer laufenden Abfrage	Write		redshift-data:statement-owner-iam-userid	
DescribeStatement	Gewährt die Berechtigung zum Abrufen detaillierter Informationen über eine Anweisungsausführung	Read		redshift-data:statement-owner-iam-userid	
DescribeTable	Gewährt die Berechtigung zum Abrufen von Metadaten zu einer bestimmten Tabelle	Read	cluster*		
			workgroup* –		
ExecuteStatement	Gewährt die Berechtigung zum Ausführen einer Abfrage	Write	cluster*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			workgroup*		
GetStatementResult	Gewährt die Berechtigung zum Abrufen des Ergebnisses einer Abfrage	Read		redshift-data:statement-owner-iam-userid	
ListDatabases	Gewährt die Berechtigung zum Auflisten von Datenbanken für einen bestimmten Cluster	Read	cluster*		
			workgroup*		
ListSchemas	Gewährt die Berechtigung zum Auflisten von Schemas für einen bestimmten Cluster	Read	cluster*		
			workgroup*		
ListStatements	Gewährt die Berechtigung zum Auflisten von Abfragen für einen bestimmten Prinzipal	List		redshift-data:statement-owner-iam-userid	
ListTables	Gewährt die Berechtigung zum Auflisten von Tabellen für einen bestimmten Cluster	List	cluster*		
			workgroup*		

Von der Amazon Redshift-Daten-API definierte Ressourcen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
cluster	`arn:${Partition}:redshift:${Region}:${Account}:cluster:${ClusterName}`	aws:ResourceTag/${TagKey}
workgroup	`arn:${Partition}:redshift-serverless:${Region}:${Account}:workgroup/${WorkgroupId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für die Amazon Redshift-Daten-API

Die Amazon-Redshift-Daten-API definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Tag-Wert, der der Ressource zugeordnet ist	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
redshift-data:statement-owner-iam-userid	Filtert den Zugriff nach Aussageninhaber iam Benutzer-ID	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Redshift Serverless

Amazon Redshift Serverless (Servicepräfix: `redshift-serverless`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Redshift Serverless definierte Aktionen
- Von Amazon Redshift Serverless definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Redshift Serverless

Von Amazon Redshift Serverless definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ConvertRecoveryPointToSnapshot	So konvertieren Sie einen Wiederherstellungspunkt in einen Snapshot	Schreiben	recoveryPoint*		
			snapshot*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomDomainAssociation	Gewährt die Berechtigung zum Erstellen einer benutzerdefinierten Domain-Zuordnung in Amazon Redshift Serverless	Schreiben	workgroup*		acm:DescribeCertificate
CreateEndpointAccess	Gewährt die Berechtigung zum Erstellen eines von Amazon Redshift Serverless verwalteten VPC-Endpunkts	Schreiben	endpointAccess*		
CreateNamespace	Erteilt die Berechtigung zum Erstellen eines Amazon Redshift Serverless-Namespace ohne Server	Schreiben	namespace*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScheduledAction	Gewährt die Berechtigung zum Erstellen einer geplanten Aktion für einen angegebenen Amazon Redshift Serverless-Namespace	Schreiben	namespace*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSnapshot	Gewährt die Berechtigung zum Erstellen eines Snapshots aller Datenbanken eines Namespace	Schreiben	snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshotCopyConfiguration	Gewährt die Berechtigung zum Erstellen einer Snapshot-Kopier-Konfiguration für einen angegebenen Amazon Redshift Serverless-Namespace	Schreiben	namespace*		
CreateUsageLimit	Erteilt die Berechtigung zum Erstellen eines Nutzungslimits für einen angegebenen Amazon Redshift Serverless-Anwendungstyp ohne Server	Schreiben			
CreateWorkgroup	Erteilt die Berechtigung zum Erstellen einer Arbeitsgruppe in Amazon Redshift Serverless	Schreiben	workgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteCustomDomainAssociation	Gewährt die Berechtigung zum Löschen einer benutzerdefinierten Domain-Zuordnung	Schreiben	workgroup*		
DeleteEndpointAccess	Gewährt die Berechtigung zum Löschen eines von Amazon Redshift Serverless verwalteten VPC-Endpunkts	Schreiben	endpointAccess*		
DeleteNamespace	Erteilt die Berechtigung zum Löschen eines Namespace aus Amazon Redshift Serverless	Schreiben	namespace*		
DeleteResourcePolicy	Gewährt die Berechtigung zum Löschen der angegebenen Tags für eine Ressource	Schreiben			
DeleteScheduledAction	Gewährt die Berechtigung zum Löschen einer geplanten Aktion aus Amazon Redshift Serverless	Schreiben			
DeleteSnapshot	Erteilt die Berechtigung zum Löschen eines Snapshots aus Amazon Redshift Serverless	Schreiben	snapshot*		
DeleteSnapshotCopyConfiguration	Gewährt die Berechtigung zum Löschen einer Snapshot-Kopier-Berechtigung für einen Amazon Redshift Serverless-Namespace	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteUsageLimit	Erteilt die Berechtigung zum Löschen eines Nutzungslimits von Amazon Redshift Serverless	Schreiben			
DeleteWorkgroup	Gewährt die Berechtigung zum Löschen einer Arbeitsgruppe	Schreiben	workgroup*		
DescribeOneTimeCredit [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen der verbleibenden Anzahl an kostenlosen Testguthaben und deren Ablaufdatum auf der Amazon-Redshift-Serverless-Konsole	Lesen			
GetCredentials	Erteilt die Berechtigung zum Abrufen eines Datenbankbenutzernamens und eines temporären Kennworts mit temporärer Berechtigung zur Anmeldung bei Amazon Redshift Serverless	Schreiben	workgroup*		
GetCustomDomainAssociation	Gewährt die Berechtigung zum Abrufen von Informationen zu einer benutzerdefinierten Domain-Zuordnung	Lesen	workgroup*		
GetEndpointAccess	Gewährt die Berechtigung zum Erstellen eines von Amazon Redshift Serverless verwalteten VPC-Endpunkts	Lesen	endpointAccess*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetNamespace	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Namespace in Amazon Redshift Serverless	Lesen	namespace*		
GetRecoveryPoint	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Wiederherstellungsgruppe	Lesen	recoveryPoint*		
GetResourcePolicy	Gewährt die Berechtigung zum Hinzufügen einer Ressourcenrichtlinie	Lesen			
GetScheduledAction	Gewährt die Berechtigung zum Abrufen von Informationen zu einer spezifischen geplanten Aktion	Lesen			
GetSnapshot	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Festplattensnapshot	Lesen	snapshot*		
GetTableRestoreStatus	Gewährt die Berechtigung zum Erhalten des Tabellenwiederherstellungsstatus zu einem spezifischen Snapshot	Lesen			
GetUsageLimit	Erteilt die Berechtigung zum Abrufen von Informationen über ein Nutzungslimit in Amazon Redshift Serverless	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetWorkgroup	Gewährt die Berechtigung zum Abrufen von Informationen zu einer bestimmten Identität	Lesen	workgroup*		
ListCustomDomainAssociations	Gewährt die Berechtigung zum Auflisten benutzerdefinierter Domain-Zuordnungen in Amazon Redshift Serverless	Auflisten			
ListEndpointAccess	Gewährt die Berechtigung zum Auflisten von EndPointAccess-Objekten und relevanten	Auflisten	endpointAccess*		
ListNamespaces	Erteilt die Berechtigung zum Auflisten von Namespaces in Amazon Redshift Serverless	Auflisten			
ListRecoveryPoints	Gewährt die Berechtigung zum Auflisten von Wiederherstellungspunkten für eine Ressource	Auflisten	namespace		
ListScheduledActions	Gewährt die Berechtigung zum Auflisten von geplanten Aktionen	Auflisten			
ListSnapshotCopyConfigurations	Gewährt die Berechtigung zum Auflisten von SnapshotCopyConfiguration-Objekten und relevanten Informationen	Auflisten	namespace		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListSnapshots	Gewährt die Berechtigung, Snapshots aufzulisten	Auflisten	snapshot*		
ListTableRestoreStatus	Gewährt die Berechtigung zum Auflisten des Tabellenwiederherstellungsstatus	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags (Metadaten), die einer Ressource zugewiesen sind	Auflisten	namespace		
			workgroup		
				aws:ResourceTag/${TagKey}	
ListUsageLimits	Erteilt die Berechtigung zum Auflisten aller Nutzungsbeschränkungen innerhalb von Amazon Redshift Serverless	Auflisten			
ListWorkgroups	Erteilt die Berechtigung zum Auflisten von Arbeitsgruppen in Amazon Redshift Serverless	Auflisten			
PutResourcePolicy	Gewährt die Berechtigung zum Erstellen oder Aktualisieren einer Ressourcenrichtlinie	Schreiben			
RestoreFromRecoveryPoint	Erteilt die Berechtigung zum Wiederherstellen der Daten von einem Wiederherstellungspunkt	Schreiben	recoveryPoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RestoreFromSnapshot	Gewährt die Berechtigung zum Wiederherstellen des Volume-Zustands aus einem Snapshot	Schreiben	snapshot*		
RestoreTableFromRecoveryPoint	Gewährt die Berechtigung zum Wiederherstellen einer Tabelle von einem Wiederherstellungspunkt	Schreiben	namespace*		
			recoveryPoint*		
RestoreTableFromSnapshot	Gewährt die Berechtigung zum Wiederherstellen einer Tabelle aus einem Snapshot	Schreiben	namespace*		
			snapshot*		
TagResource	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Tags zu einer Ressource	Markierung	namespace		
			recoveryPoint		
			snapshot		
			workgroup		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Gewährt die Berechtigung, ein oder mehrere Tags aus einer Ressource zu entfernen	Markierung	namespace		
			recoveryPoint		
			snapshot		
			workgroup		
				aws:TagKeys	
UpdateCustomDomainAssociation	Gewährt die Berechtigung zum Aktualisieren eines Zertifikats, das einer benutzerdefinierten Domain zugeordnet ist	Schreiben	workgroup*		acm:DescribeCertificate
UpdateEndpointAccess	Erteilt die Berechtigung zum Aktualisieren eines von Amazon Redshift Serverless gemanagten VPC-Endpunkts	Schreiben	endpointAccess*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateNamespace	Gewährt die Berechtigung zum Aktualisieren eines Namespace mit den angegebenen Konfigurationseinstellungen	Schreiben	namespace*		
UpdateScheduledAction	Gewährt die Berechtigung zum Aktualisieren einer geplanten Aktion	Schreiben			
UpdateSnapshot	Gewährt die Berechtigung zum Aktualisieren der Metadaten eines Snapshots	Schreiben	snapshot*		
UpdateSnapshotCopyConfiguration	Gewährt die Berechtigung zum Aktualisieren der Snapshot-Kopier-Konfiguration für einen Amazon Redshift Serverless-Namespace	Schreiben			
UpdateUsageLimit	Erteilt die Berechtigung zum Aktualisieren eines Nutzungslimits in Amazon Redshift Serverless	Schreiben			
UpdateWorkgroup	Erteilt die Berechtigung zum Aktualisieren einer Amazon Redshift Serverless-Arbeitsgruppe ohne Server mit den angegebenen Konfigurationseinstellungen	Schreiben	workgroup*		

Von Amazon Redshift Serverless definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
namespace	`arn:${Partition}:redshift-serverless:${Region}:${Account}:namespace/${NamespaceId}`	aws:ResourceTag/${TagKey}
snapshot	`arn:${Partition}:redshift-serverless:${Region}:${Account}:snapshot/${SnapshotId}`	aws:ResourceTag/${TagKey}
workgroup	`arn:${Partition}:redshift-serverless:${Region}:${Account}:workgroup/${WorkgroupId}`	aws:ResourceTag/${TagKey}
recoveryPoint	`arn:${Partition}:redshift-serverless:${Region}:${Account}:recoverypoint/${RecoveryPointId}`	aws:ResourceTag/${TagKey}
endpointAccess	`arn:${Partition}:redshift-serverless:${Region}:${Account}:managedvpcendpoint/${EndpointAccessId}`	

Bedingungsschlüssel für Amazon Redshift Serverless

Amazon Redshift Serverless definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString
redshift-serverless:endpointAccessId	Filtert den Zugriff nach der Kennung der Aktion	Zeichenfolge
redshift-serverless:namespaceId	Filtert den Zugriff nach der Kennung der Aktion	Zeichenfolge
redshift-serverless:recoveryPointId	Filtert den Zugriff nach der Kennung des Wiederherstell	Zeichenfolge
redshift-serverless:snapshotId	Filtert den Zugriff nach der Kennung der Aktion	Zeichenfolge
redshift-serverless:tableRestoreRequestId	Filtert den Zugriff nach der Kennung der Tabellenwiederherstellungsanforderung	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
redshift-serverless:workgroupId	Filtert den Zugriff nach der Kennung des Workers	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Rekognition

Amazon Rekognition (Servicepräfix: `rekognition`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Rekognition definierte Aktionen
- Von Amazon Rekognition definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Rekognition

Von Amazon Rekognition definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt,

müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateFaces	Gewährt die Berechtigung, mehrere individuelle Gesichter einem einzelnen Benutzer zuzuordnen	Schreiben	collection*		
CompareFaces	Gewährt die Berechtigung zum Vergleichen von	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Gesichtern im Eingabebild der Quelle mit jedem Gesicht, das im Eingabebild des Ziels erkannt wurde				
CopyProjectVersion	Gewährt die Berechtigung zum Kopieren einer vorhandenen Modellversion in eine neue Modellversion.	Schreiben	project*		
			projectversion*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCollection	Gewährt die Berechtigung zum Erstellen einer Sammlung in einer AWS-Region	Schreiben	collection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataset	Gewährt die Berechtigung zum Erstellen eines neuen Amazon-Rekognition-Custom-Labels-Datensatzes	Schreiben	project*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateFaceLivenessSession	Gewährt die Berechtigung zum Erstellen einer Face-Liveness-Sitzung	Schreiben			
CreateProject	Gewährt die Berechtigung zum Erstellen eines Amazon-Rekognition-Custom-Labels-Projekts	Schreiben	project*		
CreateProjectVersion	Gewährt die Berechtigung, mit dem Training einer neuen Version eines Modells zu beginnen	Schreiben	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStreamProcessor	Gewährt die Berechtigung zum Erstellen eines Amazon-Rekognition-Stream-Prozessors	Schreiben	collection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUser	Gewährt die Berechtigung zum Erstellen eines neuen Benutzers in einer Sammlung mithilfe einer eindeutigen Benutzer-ID, die Sie angeben	Schreiben	collection*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteCollection	Gewährt die Berechtigung zum Löschen der angegebenen Sammlung	Schreiben	collection*		
DeleteDataset	Gewährt die Berechtigung zum Löschen eines bestehenden Amazon-Rekognition-Custom-Labels-Datensatzes	Schreiben	dataset*		
DeleteFaces	Gewährt die Berechtigung zum Löschen von Gesichtern aus einer Sammlung	Schreiben	collection*		
DeleteProject	Gewährt die Berechtigung zum Löschen eines Projekts	Schreiben	project*		
DeleteProjectPolicy	Gewährt die Berechtigung zum Löschen einer Ressourcenrichtlinie, die an ein Projekt angefügt ist.	Schreiben	project*		
DeleteProjectVersion	Gewährt die Berechtigung zum Löschen eines Trails	Schreiben	projectversion*		
DeleteStreamProcessor	Gewährt die Berechtigung zum Löschen des angegebenen Stream-Prozessors	Schreiben	streamprocessor*		
DeleteUser	Gewährt die Berechtigung zum Löschen eines Benutzers aus der Sammlung basierend auf der angegebenen Benutzer-ID	Schreiben	collection*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeCollection	Gewährt die Berechtigung zum Lesen von Details über eine Sammlung	Lesen	collection*		
DescribeDataset	Gewährt die Berechtigung zum Beschreiben eines Amazon-Rekognition-Custom-Labels-Datensatzes	Lesen	dataset*		
DescribeProjectVersions	Gewährt die Berechtigung zum Auflisten der Versionen eines Modells in einem Amazon-Rekognition-Custom-Labels-Projekt	Lesen	project*		
DescribeProjects	Gewährt die Berechtigung zum Auflisten von Amazon-Rekognition-Custom-Labels-Projekten	Lesen			
DescribeStreamProcessor	Gewährt die Berechtigung zum Abrufen von Informationen über den angegebenen Stream-Prozessor	Lesen	streamprocessor*		
DetectCustomLabels	Gewährt die Berechtigung zum Erkennen benutzerdefinierter Labels in einem bereitgestellten Bild	Lesen	projectversion*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DetectFaces	Gewährt die Berechtigung, menschliche Gesichter in einem Bild zu erkennen, das als Eingabe bereitgestellt wird	Lesen			
DetectLabels	Gewährt die Berechtigung zum Erkennen von Vorkommnissen von realen Markierungen in einem als Eingabe bereitgestellten Bild	Lesen			
DetectModerationLabels	Gewährt die Berechtigung zum Erkennen von Moderations-Markierungen im Eingabebild	Lesen	projectversion		
DetectProtectiveEquipment	Gewährt die Berechtigung zum Erkennen persönlicher Schutzausrüstung im Eingabebild	Lesen			
DetectText	Gewährt die Berechtigung zum Erkennen von Text im Eingangsbild und konvertiert diesen in maschinenlesbaren Text	Lesen			
DisassociateFaces	Gewährt die Berechtigung zum Löschen der Verknüpfung zwischen einer Benutzer-ID und einer Gesichts-ID	Schreiben	collection*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DistributeDatasetEntries	Gewährt die Berechtigung zum Verteilen der Einträge in einem Trainings-Datensatz über den Trainings-Datensatz und den Test-Datensatz für ein Projekt	Schreiben	dataset*		
GetCelebrityInfo	Gewährt die Berechtigung, den Namen und zusätzliche Informationen eines Prominenten zu lesen	Lesen			
GetCelebrityRecognition	Gewährt die Berechtigung zum Lesen der Erkennungs-Ergebnisse des Prominenten, die in einem gespeicherten Video von einem asynchronen Prominenten-Erkennungs-Auftrag gefunden wurden	Lesen			
GetContentModeration	Gewährt die Berechtigung, die Ergebnisse der Inhaltsmoderations-Analyse zu lesen, die in einem gespeicherten Video durch einen asynchronen Auftrag zur Inhaltsmoderation gefunden wurden	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetFaceDetection	Gewährt die Berechtigung zum Lesen der Gesichterkennungs-Ergebnisse, die in einem gespeicherten Video durch einen asynchronen Gesichtserkennungs-Auftrag gefunden wurden	Lesen			
GetFaceLivenessSessionResults	Gewährt die Berechtigung zum Abrufen der Ergebnisse einer Face-Liveness-Sitzung	Lesen			
GetFaceSearch	Gewährt die Berechtigung zum Lesen der übereinstimmenden Sammlungsgesichter, die in einem gespeicherten Video von einem asynchronen Gesichter-Suchauftrag gefunden wurden	Lesen			
GetLabelDetection	Gewährt die Berechtigung zum Lesen der Markierungs-Erkennungs-Ergebnisse, die in einem gespeicherten Video durch einen asynchronen Markierungs-Erkennungs-Auftrag gefunden wurden	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetMediaAnalysisJob	Gewährt die Berechtigung zum Lesen des Verweises auf Auftragsergebnisse in S3 und zusätzlicher Informationen zu einem Medienanalyseauftrag	Lesen			
GetPersonTracking	Gewährt die Berechtigung, die Liste der Personen zu lesen, die in einem gespeicherten Video von einem asynchronen Personenverfolgungs-Auftrag entdeckt wurden	Lesen			
GetSegmentDetection	Gewährt die Berechtigung, die Video-Segmente abzurufen , die in einem gespeicherten Video durch einen asynchronen Segmenterkennungs-Auftrag gefunden wurden	Lesen			
GetTextDetection	Gewährt die Berechtigung, den Text abzurufen, der in einem gespeicherten Video durch einen asynchronen Texterkennungs-Auftrag gefunden wurde	Lesen			
IndexFaces	Gewährt die Berechtigung zum Aktualisieren einer vorhandenen Sammlung mit Gesichtern, die im Eingabebild erkannt wurden	Schreiben	collection*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListCollections	Gewährt die Berechtigung, die Sammlungs-IDs in Ihrem Konto zu lesen	Lesen			
ListDatasetEntries	Gewährt die Berechtigung, die Datensatzeinträge in einem bestehenden Amazon-Rekognition-Custom-Labels-Datensatz aufzulisten	Lesen	dataset*		
ListDatasetLabels	Gewährt die Berechtigung zum Auflisten der Markierungen in einem Datensatz	Lesen	dataset*		
ListFaces	Gewährt die Berechtigung zum Lesen von Metadaten für Gesichter in der angegebenen Sammlung	Lesen	collection*		
ListMediaAnalysisJobs	Gewährt die Berechtigung zum Lesen der Liste der Medienanalyseaufträge	Lesen			
ListProjectPolicies	Gewährt die Berechtigung zum Auflisten der Ressourcenrichtlinie, die an ein Projekt angefügt ist.	Lesen	project*		
ListStreamProcessors	Gewährt die Berechtigung zum Abrufen einer Liste Ihrer Stream-Prozessoren	Auflisten	streamprocessor*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Abrufen einer Liste von Tags, die einer Ressource zugeordnet sind	Lesen	projectversion*		
ListUsers	Gewährt die Berechtigung zum Auflisten von UserIds und dem UserStatus	Lesen	collection*		
PutProjectPolicy	Gewährt die Berechtigung zum Anfügen einer Ressourcenrichtlinie an ein Projekt.	Schreiben	project*		
RecognizeCelebrities	Gewährt die Berechtigung zum Erkennen von Prominenten im Eingabebild	Lesen			
SearchFaces	Gewährt die Berechtigung, die spezifische Sammlung nach der bereitgestellten Gesichts-ID zu durchsuchen	Lesen	collection*		
SearchFacesByImage	Gewährt die Berechtigung, die spezifische Sammlung nach dem größten Gesicht im Eingabebild zu durchsuchen	Lesen	collection*		
SearchUsers	Gewährt die Berechtigung, die spezifische Sammlung nach Benutzerübereinstimmungsergebnissen mit der angegebenen Gesichts-ID oder Benutzer-ID zu durchsuchen	Lesen	collection*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SearchUsersByImage	Gewährt die Berechtigung, die spezifische Sammlung nach Benutzerübereinstimmungsergebnissen mit dem größten Gesicht im Eingabebild zu durchsuchen	Lesen	collection*		
StartCelebrityRecognition	Gewährt die Berechtigung, die asynchrone Erkennung von Prominenten in einem gespeicherten Video zu starten	Schreiben			
StartContentModeration	Gewährt die Berechtigung zum Starten der asynchronen Erkennung von expliziten oder provokanten nicht jugendfreien Inhalten in einem gespeicherten Video	Schreiben			
StartFaceDetection	Gewährt die Berechtigung zum Starten der asynchronen Erkennung von Gesichtern in einem gespeicherten Video	Schreiben			
StartFaceLivenessSession	Gewährt die Berechtigung zum Starten von Video-Streaming für eine Face-Liveness-Sitzung	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartFaceSearch	Gewährt die Berechtigung zum Starten der asynchronen Suche nach Gesichtern in einer Sammlung, die den Gesichtern von in einem gespeicherten Video erkannten Personen entsprechen	Schreiben	collection*		
StartLabelDetection	Gewährt die Berechtigung zum Starten der asynchronen Erkennung von Markierungen in einem gespeicherten Video	Schreiben			
StartMediaAnalysisJob	Gewährt die Berechtigung zum Starten eines Medienanalyseauftrags	Schreiben	projectversion		
StartPersonTracking	Gewährt die Berechtigung zum Starten der asynchronen Verfolgung von Personen in einem gespeicherten Video	Schreiben			
StartProjectVersion	Gewährt die Berechtigung zum Starten einer Modellversion	Schreiben	projectversion*		
StartSegmentDetection	Gewährt die Berechtigung zum Starten der asynchronen Erkennung von Segmenten in einem gespeicherten Video	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartStreamProcessor	Gewährt die Berechtigung zum Starten eines Stream-Prozessors	Schreiben	streamprocessor*		
StartTextDetection	Gewährt die Berechtigung zum Starten der asynchronen Erkennung von Text in einem gespeicherten Video	Schreiben			
StopProjectVersion	Gewährt die Berechtigung zum Beenden einer laufenden Modellversion	Schreiben	projectversion*		
StopStreamProcessor	Gewährt die Berechtigung zum Beenden eines laufenden Stream-Prozessors	Schreiben	streamprocessor*		
TagResource	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Tags zu einer Ressource	Markieren	collection		
			projectversion		
			streamprocessor		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource		Markierung	collection		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Gewährt die Berechtigung, ein oder mehrere Tags aus einer Ressource zu entfernen		projectversion		
			streamprocessor		
				aws:TagKeys	
UpdateDatasetEntries	Gewährt die Berechtigung zum Hinzufügen oder Aktualisieren einer oder mehrerer JSON-Linien (Einträge) in einem Datensatz	Schreiben	dataset*		
UpdateStreamProcessor	Erteilt die Berechtigung zum Ändern von Eigenschaften für einen Stream-Prozessor	Schreiben	streamprocessor*		

Von Amazon Rekognition definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
collection	`arn:${Partition}:rekognition:${Region}:${Account}:collection/${CollectionId}`	aws:ResourceTag/${TagKey}
streamprocessor	`arn:${Partition}:rekognition:${Region}:${Account}:streamprocessor/${StreamprocessorId}`	aws:ResourceTag/${TagKey}
project	`arn:${Partition}:rekognition:${Region}:${Account}:project/${ProjectName}/${CreationTimestamp}`	
projectversion	`arn:${Partition}:rekognition:${Region}:${Account}:project/${ProjectName}/version/${VersionName}/${CreationTimestamp}`	aws:ResourceTag/${TagKey}
dataset	`arn:${Partition}:rekognition:${Region}:${Account}:project/${ProjectName}/dataset/${DatasetType}/${CreationTimestamp}`	

Bedingungsschlüssel für Amazon Rekognition

Amazon Rekognition definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch Tags, die in der Anforderung übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf Tags, die der Ressource zugeordnet sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf Tag-Schlüsseln, die in der Anforderung übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Resilience Hub

AWS Resilience Hub (Dienstpräfix:`resiliencehub`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Resilience Hub definierte Aktionen
- Von AWS Resilience Hub definierte Ressourcentypen
- Bedingungsschlüssel für AWS Resilience Hub

Von AWS Resilience Hub definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen.

Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddDraftAppVersionResourceMappings	Gewährt die Berechtigung zum Hinzufügen von Ressourcen-Zuordnungen für die Anwendungsversion	Schreiben	application*		cloudformation:DescribeStacks cloudformation:ListStackResources resource-groups:GetGroup resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog:ListAssociatedResources
BatchUpdateRecommendationStatus	Erteilt die Berechtigung, eine oder mehrere betriebliche	Schreiben	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Empfehlungen aufzunehmen oder auszuschließen				
CreateApp	Gewährt die Berechtigung zum Erstellen einer Anwendung	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAppVersionAppComponent	Gewährt die Berechtigung zum Erstellen einer Anwendungs-App-Komponente	Schreiben	application*		
CreateAppVersionResource	Gewährt die Berechtigung zum Erstellen einer Anwendungsressource	Schreiben	application*		
CreateRecommendationTemplate	Gewährt die Berechtigung zum Erstellen einer Empfehlungs-Vorlage	Schreiben	application*		s3:CreateBucket s3:ListBucket s3:PutObject
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateResiliencyPolicy	Gewährt die Berechtigung zum Erstellen einer Ausfallsicherheit-Richtlinie	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApp	Gewährt die Berechtigung zum Löschen von Anwendungen im Batch	Schreiben	application*		
DeleteAppAssessment	Gewährt die Berechtigung zum Löschen von Anwendungs-Bewertungen im Batch	Schreiben	application*		
DeleteAppInputSource	Gewährt die Berechtigung zum Entfernen einer Anwendungseingabequelle.	Schreiben	application*		
DeleteAppVersionAppComponent	Gewährt die Berechtigung zum Löschen einer Anwendungs-App-Komponente	Schreiben	application*		
DeleteAppVersionResource	Gewährt die Berechtigung zum Löschen einer Anwendungsressource	Schreiben	application*		
DeleteRecommendationTemplate	Gewährt die Berechtigung zum Löschen von Empfehlungs-Vorlagen im Batch	Schreiben	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteResiliencyPolicy	Gewährt die Berechtigung zum Löschen von Ausfallsicherheit-Richtlinien im Batch	Schreiben	resiliency-policy*		
DescribeApp	Gewährt die Berechtigung zum Beschreiben einer Anwendung	Lesen	application*		
DescribeAppAssessment	Gewährt die Berechtigung zum Beschreiben einer Anwendungs-Bewertung	Lesen	application*		
DescribeAppVersion	Gewährt die Berechtigung zum Beschreiben einer Anwendungsversion	Lesen	application*		
DescribeAppVersionAppComponent	Gewährt die Berechtigung zum Beschreiben einer App-Komponente der Anwendungsversion	Lesen	application*		
DescribeAppVersionResource	Gewährt die Berechtigung zum Beschreiben einer Anwendungsversionsressource	Lesen	application*		
DescribeAppVersionResourcesResolutionStatus	Gewährt die Berechtigung zum Beschreiben einer Anwendungs-Auflösung	Lesen	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeAppVersionTemplate	Gewährt die Berechtigung zum Beschreiben einer Anwendungsversions-Vorlage	Lesen	application*		
DescribeDraftAppVersionResourcesImportStatus	Gewährt die Berechtigung zum Beschreiben des Importstatus von Ressourcen für den Entwurf einer Anwendungsversion	Lesen	application*		
DescribeResiliencyPolicy	Gewährt die Berechtigung zum Beschreiben einer Ausfallsicherheit-Richtlinie	Lesen	resiliency-policy*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ImportResourcesToDraftAppVersion	Gewährt die Berechtigung zum Importieren von Ressourcen für den Entwurf einer Anwendungsversion	Schreiben	application*		cloudformation:DescribeStacks cloudformation:ListStackResources resource-groups:GetGroup resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog:ListAssociatedResources
ListAlarmRecommendations	Gewährt die Berechtigung zum Auflisten von Alarm-Empfehlungen	Auflisten	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAppAssessmentComplianceDrifts	Erteilt die Berechtigung, Konformitätsabweichungen aufzulisten, die bei der Durchführung einer Bewertung festgestellt wurden	Auflisten	application*		
ListAppAssessmentResourceDrifts	Erteilt die Berechtigung, Ressourcenabweichungen aufzulisten, die bei der Ausführung einer Bewertung festgestellt wurden	Auflisten	application*		
ListAppAssessments	Gewährt die Berechtigung zum Auflisten von Anwendungs-Bewertungen	Auflisten			
ListAppComponentCompliances	Gewährt die Berechtigung zum Auflisten der Compliance von Komponenten einer App	Auflisten	application*		
ListAppComponentRecommendations	Gewährt die Berechtigung zum Auflisten von Empfehlungen für App-Komponenten	Auflisten	application*		
ListAppInputSources	Gewährt die Berechtigung zum Auflisten der Anwendungseingaberessourcen	Auflisten	application*		
ListAppVersionAppComponents	Gewährt die Berechtigung zum Auflisten von App-Komponenten der Anwendungsversion	Auflisten	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAppVersionResourceMappings	Gewährt Berechtigung für Ressourcen-Mappings der Anwendungsversion	Auflisten	application*		
ListAppVersionResources	Gewährt die Berechtigung zum Auflisten der Ressourcen einer Anwendung	Auflisten	application*		
ListAppVersions	Gewährt die Berechtigung zum Auflisten der Anwendungsversion	Auflisten	application*		
ListApps	Gewährt die Berechtigung zum Auflisten von Anwendungen	Auflisten			
ListRecommendationTemplates	Gewährt die Berechtigung zum Auflisten von Empfehlungs-Vorlagen	Auflisten	application*		
ListResiliencyPolicies	Gewährt die Erlaubnis zum Auflisten von Ausfallsicherheits-Richtlinien	Auflisten			
ListSopRecommendations	Gewährt die Berechtigung zum Auflisten von SOP-Empfehlungen	Auflisten	application*		
ListSuggestedResiliencyPolicies	Gewährt die Berechtigung zum Empfehlen von Ausfallsicherheits-Richtlinien	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen			
ListTestRecommendations	Gewährt die Berechtigung zum Auflisten von Test-Empfehlungen	Auflisten	application*		
ListUnsupportedAppVersionResources	Gewährt Berechtigung zum Auflisten von nicht unterstützten Ressourcen der Anwendungsversion	Auflisten	application*		
PublishAppVersion	Gewährt die Berechtigung zum Veröffentlichen der Anwendungsversion	Schreiben	application*		
PutDraftAppVersionTemplate	Gewährt die Berechtigung zum Ablegen des Entwurfs einer Anwendungsversions-Vorlage	Schreiben	application*		
RemoveDraftAppVersionResourceMappings	Gewährt die Berechtigung zum Entfernen von Mappings für die Anwendungsversion	Schreiben	application*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ResolveAppVersionResources	Gewährt Berechtigung zum Auflösen von Ressourcen der Anwendungsversion	Schreiben	application*		cloudformation:DescribeStacks cloudformation:ListStackResources resource-groups:GetGroup resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog:ListAssociatedResources

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartAppAssessment	Gewährt die Berechtigung zum Erstellen einer Anwendungs-Bewertung	Schreiben	application*		cloudformation:DescribeStacks cloudformation:ListStackResources cloudwatch:DescribeAlarms cloudwatch:GetMetricData cloudwatch:GetMetricStatistics cloudwatch:PutMetricData ec2:DescribeRegions fis:GetExperimentTemplate

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					fis:ListExperimentTemplates fis:ListExperiments resource-groups:GetGroup resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog:ListAssociatedResources ssm:GetParametersByPath

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Gewährt die Berechtigung zum Zuordnen eines Ressourcen-Tags.	Tagging	app-assessment		
			application		
			recommendation-template		
			resiliency-policy		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Tagging	app-assessment		
			application		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			recommendation-template		
			resiliency-policy		
				aws:TagKeys	
UpdateApp	Gewährt die Berechtigung zum Aktualisieren einer Anwendung	Schreiben	application*		
UpdateAppVersion	Gewährt die Berechtigung zum Aktualisieren einer Anwendungsversion	Schreiben	application*		
UpdateAppVersionAppComponent	Gewährt die Berechtigung zum Aktualisieren einer Anwendungs-App-Komponente	Schreiben	application*		
UpdateAppVersionResource	Gewährt die Berechtigung zum Aktualisieren einer Anwendungsressource	Schreiben	application*		
UpdateResiliencyPolicy	Gewährt die Berechtigung zum Aktualisieren einer Ausfallsicherheits-Richtlinie	Schreiben	resiliency-policy*		

Von AWS Resilience Hub definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
resiliency-policy	`arn:${Partition}:resiliencehub:${Region}:${Account}:resiliency-policy/${ResiliencyPolicyId}`	aws:ResourceTag/${TagKey}
application	`arn:${Partition}:resiliencehub:${Region}:${Account}:app/${AppId}`	aws:ResourceTag/${TagKey}
app-assessment	`arn:${Partition}:resiliencehub:${Region}:${Account}:app-assessment/${AppAssessmentId}`	aws:ResourceTag/${TagKey}
recommendation-template	`arn:${Partition}:resiliencehub:${Region}:${Account}:recommendation-template/${RecommendationTemplateId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Resilience Hub

AWS Resilience Hub definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	String
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Resource Access Manager (RAM)

AWS Resource Access Manager (RAM) (Servicepräfix: `ram`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Resource Access Manager (RAM) definierte Aktionen
- Von AWS Resource Access Manager (RAM) definierte Ressourcentypen
- Bedingungsschlüssel für AWS Resource Access Manager (RAM)

Von AWS Resource Access Manager (RAM) definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWSzu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptResourceShareInvitation	Gewährt die Berechtigung zum Akzeptieren der angegebenen Ressourcenfreigabe	Write	resource-share-invitation*		
				ram:ShareOwnerAccountId ram:ResourceShareName	
AssociateResourceShare	Gewährt die Berechtigung, Ressourcen und/oder Prinzipale einer Ressourcenfreigabe zuzuordnen	Write	resource-share*		
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:Principal	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ram:RequestedResourceType ram:ResourceArn	
AssociateResourceSharePermission	Gewährt die Berechtigung, eine Berechtigung mit einer Ressourcenfreigabe zu verknüpfen	Schreiben	customer-managed-permission*		
			permission*		
			resource-share*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreatePermission	Gewährt die Berechtigung, eine Berechtigung zu erstellen, die mit einer Ressourcenfreigabe verknüpft werden kann	Schreiben		ram:PermissionArn ram:PermissionResourceType aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	ram:TagResource
CreatePermissionVersion	Gewährt die Berechtigung, eine neue Version einer Berechtigung zu erstellen, die mit einer Ressourcenfreigabe verknüpft werden kann	Schreiben	customer-managed-permission*		
				ram:PermissionArn ram:PermissionResourceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateResourceShare	Gewährt die Berechtigung zum Erstellen einer Ressourcenfreigabe mit bereitgestellten Ressourcen und/oder Prinzipalen	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys ram:RequestedResourceType ram:ResourceArn ram:RequestedAllowsExternalPrincipals ram:Principal	
DeletePermission	Gewährt die Berechtigung zum Löschen einer angegebenen Berechtigung	Schreiben	customer-managed-permission*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} ram:PermissionArn ram:PermissionResourceType	
DeletePermissionVersion	Gewährt die Berechtigung zum Löschen einer bestimmten Version einer Berechtigung	Schreiben	customer-managed-permission*		
				ram:PermissionArn ram:PermissionResourceType	
DeleteResourceShare	Gewährt die Berechtigung zum Löschen einer Ressourcenfreigabe	Write	resource-share*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals	
DisassociateResourceShare	Gewährt die Berechtigung, Ressourcen und/oder Prinzipale von einer Ressourcenfreigabe zu trennen	Write	resource-share*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:Principal ram:RequestedResourceType ram:ResourceArn	
DisassociateResourceSharePermission	Gewährt die Berechtigung, eine Berechtigung von einer Ressourcenfreigabe zu trennen	Write	customer-managed-permission* –		
			permission*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			resource-share*		
EnableSharingWithAwsOrganization	Gewährt die Berechtigung für den Zugriff auf die Organisation des Kunden und erstellt eine SLR im Konto des Kunden	Berechtigungsverwaltung			iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:EnableAWSServiceAccess
GetPermission	Gewährt die Berechtigung zum Abrufen des Inhalts einer - AWS RAM-Berechtigung	Lesen	customer-managed-permission*		
			permission*		
				ram:PermissionArn	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetResourcePolicies	Gewährt die Berechtigung zum Abrufen der Richtlinien für die angegebenen Ressourcen, die Sie besitzen und freigegeben haben	Read			
GetResourceShareAssociations	Gewährt die Berechtigung zum Abrufen einer Reihe von Ressourcenfreigabemappingen von einer bereitgestellten Liste oder mit einem angegebenen Status des entsprechenden Typs	Read			
GetResourceShareInvitations	Gewährt die Berechtigung zum Abrufen von Ressourcenfreigabeeinladungen anhand des angegebenen Einladungs-ARN oder von Einladungen für die Ressourcenfreigabe	Read			
GetResourceShares	Gewährt die Berechtigung zum Abrufen einer Reihe von Ressourcenfreigaben aus einer bereitgestellten Liste oder mit einem bestimmten Status	Read		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListPendingInvitationResources	Gewährt die Berechtigung zum Auflisten der Ressourcen in einer Ressourcefreigabe auf, die zwar für Sie freigegeben wurde, aber für die die Einladung noch aussteht	Lesen	resource-share-invitation*		
				ram:ResourceShareName	
ListPermissionAssociations	Gewährt die Berechtigung zum Auflisten von Informationen über die Berechtigung und alle Verknüpfungen	Auflisten	customer-managed-permission*		
			permission*		
				ram:PermissionArn ram:PermissionResourceType	
ListPermissionVersions	Gewährt die Berechtigung zum Auflisten der Versionen einer - AWS RAM-Berechtigung	Auflisten			
ListPermissions	Gewährt die Berechtigung zum Auflisten der AWS RAM-Berechtigungen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListPrincipals	Gewährt die Berechtigung zum Auflisten der Prinzipale, für die Sie über freigegebene Ressourcen verfügen oder für die gemeinsam genutzte Ressourcen verwendet werden	Auflisten			
ListReplacePermissionAssociationsWork	Gewährt die Berechtigung, den Status der asynchronen Berechtigungsersetzung abzurufen	Auflisten			
ListResourceSharePermissions	Gewährt die Berechtigung zum Auflisten der mit einer Ressourcenfreigabe verbundenen Berechtigungen	Auflisten	resource-share*		
				aws:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals	
ListResourceTypes	Gewährt die Berechtigung zum Auflisten der gemeinsam nutzbaren Ressourcentypen, die von AWS RAM unterstützt werden	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListResources	Gewährt die Berechtigung zum Auflisten der Ressourcen, die Sie zu Ressourcenfreigaben hinzugefügt haben, oder die Ressourcen, die mit Ihnen geteilt werden	Auflisten			
PromotePermissionCreatedFromPolicy	Gewährt die Berechtigung zur Erstellung einer separaten, vollständig verwaltbaren kundenbezogenen Berechtigung	Schreiben	customer-managed-permission*		
				ram:PermissionArn ram:PermissionResourceType	
PromoteResourceShareCreatedFromPolicy	Gewährt die Berechtigung, die angegebene Ressourcenfreigabe zu fördern	Write	resource-share*		
RejectResourceShareInvitation	Gewährt die Berechtigung zum Ablehnen der angegebenen Ressourcenfreigabe	Schreiben	resource-share-invitation*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ram:ShareOwnerAccountId ram:ResourceShareName	
ReplacePermissionAssociations	Gewährt die Berechtigung zum Aktualisieren aller Ressourcenfreigaben auf eine neue Berechtigung	Schreiben	customer-managed-permission*		
			permission*		
				ram:PermissionArn ram:PermissionResourceType	
SetDefaultPermissionVersion	Gewährt die Berechtigung, eine Versionsnummer als Standardversion für die jeweilige vom Kunden verwaltete Berechtigung festzulegen	Schreiben	customer-managed-permission*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ram:PermissionArn ram:PermissionResourceType	
TagResource	Gewährt die Berechtigung zum Markieren der angegebenen Ressourcenfreigabe oder -Berechtigung	Tagging	customer-managed-permission		
			resource-share		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung die Markierung der angegebenen Ressourcenfreigabe oder -Berechtigung aufzuheben	Tagging	customer-managed-permission		
			resource-share		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateResourceShare	Gewährt die Berechtigung zum Aktualisieren von Attributen der Ressourcenfreigabe	Schreiben	resource-share*		
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:RequestedAllowsExternalPrincipals	

Von AWS Resource Access Manager (RAM) definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
resource-share	`arn:${Partition}:ram:${Region}:${Account}:resource-share/${ResourcePath}`	aws:ResourceTag/${TagKey} ram:AllowsExternalPrincipals ram:ResourceShareName
resource-share-invitation	`arn:${Partition}:ram:${Region}:${Account}:resource-share-invitation/${ResourcePath}`	ram:ShareOwnerAccountId
permission	`arn:${Partition}:ram::${Account}:permission/${ResourcePath}`	ram:PermissionArn ram:PermissionResourceType
customer-managed-permission	`arn:${Partition}:ram:${Region}:${Account}:permission/${ResourcePath}`	aws:ResourceTag/${TagKey} ram:PermissionArn ram:PermissionResourceType

Bedingungsschlüssel für AWS Resource Access Manager (RAM)

AWS Resource Access Manager (RAM) definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach den Tags, die in der Anfrage beim Erstellen oder Markieren einer Ressourcenfreigabe übergeben werden. Werden nicht genau diese Tags übergeben oder überhaupt keine Tags angegeben, schlägt die Anforderung fehl	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	String
aws:TagKeys	Filtert den Zugriff nach den Tag-Schlüsseln, die beim Erstellen oder Markieren einer Ressourcenfreigabe übergeben werden	ArrayOfString
ram:AllowsExternalPrincipals	Filtert den Zugriff nach den Ressourcenfreigaben, die die gemeinsame Nutzung mit externen Prinzipalen erlauben oder verweigern. Geben Sie beispielsweise „true“ an, wenn die Aktion nur für Ressourcenfreigaben ausgeführt werden kann, die die Freigabe mit externen Prinzipalen zulassen. Externe Prinzipale sind AWS Konten, die sich außerhalb ihrer AWS Organisation befinden.	Bool
ram:PermissionArn	Filtert den Zugriff nach dem angegebenen Berechtigungs-ARN	ARN
ram:PermissionResourceType	Filtert den Zugriff nach den Berechtigungen des angegebenen Ressourcentyps	String
ram:Principal	Filtert den Zugriff nach dem Format des angegebenen Prinzipals	String
ram:RequestedAllow	Filtert den Zugriff nach dem angegebenen Wert für „allowExternalPrincipals“. Externe Prinzipale sind AWS	Bool

Bedingungsschlüssel	Beschreibung	Typ
sExternalPrincipals	Konten, die sich außerhalb ihrer - AWS Organisation befinden.	
ram:RequestedResourceType	Filtert den Zugriff nach dem angegebenen Ressourcentyp	String
ram:ResourceArn	Filtert den Zugriff nach dem angegebenen ARN	ARN
ram:ResourceShareName	Filtert den Zugriff nach einer Ressourcenfreigabe mit dem angegebenen Namen	String
ram:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	String
ram:ShareOwnerAccountId	Filtert den Zugriff nach Ressourcenfreigaben, die einem bestimmten Konto gehören. Beispielsweise können Sie diesen Bedingungsschlüssel verwenden, um anzugeben, welche Ressourcefreigabeeinladungen basierend auf der Konto-ID des Eigentümers der Ressourcenfreigabe angenommen oder abgelehnt werden können	String

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Resource Explorer

AWS Resource Explorer (Servicepräfix: `resource-explorer-2`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.

- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Resource Explorer definierte Aktionen
- Von AWS Resource Explorer definierte Ressourcentypen
- Bedingungsschlüssel für AWS Resource Explorer

Von AWS Resource Explorer definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateDefaultView	Gewährt die Berechtigung zum Festlegen der angegebenen Ansicht als Standard für diese AWS-Region in diesem AWS-Konto	Schreiben	view*		
BatchGetView	Gewährt die Berechtigung zum Abrufen von Details zu Ansichten	Lesen			resource-explorer-2:GetView
CreateIndex	Gewährt die Berechtigung zum Aktivieren des Resource Explorers in der AWS-Region, in der Sie diesen Vorgang aufgerufen haben, indem Sie einen Index erstellt haben	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateView	Gewährt die Berechtigung zum Erstellen einer Ansicht	Schreiben		aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
DeleteIndex	Gewährt die Berechtigung zum Deaktivieren des Resource Explorers in der angegebenen AWS-Region, indem der Index gelöscht wird	Schreiben	index*		
DeleteView	Gewährt die Berechtigung zum Löschen einer Ansicht	Schreiben	view*		
DisassociateDefaultView	Gewährt die Berechtigung zum Entfernen der Standardansicht für die AWS-Region in der Sie diesen Vorgang aufrufen	Schreiben			
GetAccountLevelServiceConfiguration	Gewährt Resource Explorer die Erlaubnis, auf Daten auf Kontoebene innerhalb Ihrer AWS-Organisation zuzugreifen	Lesen			
GetDefaultView	Gewährt die Berechtigung zum Abrufen des Amazon-Ressourcennamens (ARN) der Ansicht, die die Standardeinstellung für die AWS-Region ist, in der Sie diesen Vorgang aufrufen	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetIndex	Gewährt die Berechtigung zum Abrufen von Informationen über den Index in der AWS-Region in der Sie diesen Vorgang aufrufen	Lesen			
GetView	Gewährt die Berechtigung zum Abrufen von Informationen zur angegebenen Ansicht	Lesen	view*		
ListIndexes	Gewährt die Berechtigung zum Auflisten der Indizes in allen AWS-Regionen	Auflisten			
ListIndexesForMembers	Gewährt die Berechtigung zum Auflisten der Konto-Indizes der Organisationsmitglieder in allen AWS-Regionen	Auflisten			
ListSupportedResourceTypes	Gewährt die Berechtigung zum Abrufen einer Liste aller von Resource Explorer unterstützten Ressourcentypen	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags, die einer bestimmten Ressource angefügt sind	Lesen	index		
			view		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListViews	Gewährt die Berechtigung zum Auflisten der Amazon-Ressourcennamen (ARNs) aller Ansichten, die in der AWS-Region verfügbar sind, in der Sie diesen Vorgang aufrufen	Auflisten			
Search	Gewährt die Berechtigung zum Suchen nach Ressourcen und zum Anzeigen von Details zu allen Ressourcen, die den angegebenen Kriterien entsprechen	Lesen	view*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von einem oder mehreren Tag-Schlüssel/Wert-Paaren der angegebenen Ressource	Markierung	index		
			view		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von einem oder mehreren Tag-Schlüssel/Wert-Paaren aus der angegebenen Ressource	Markierung	index		
			view		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateIndexType	Gewährt die Berechtigung zum Ändern des Indextyps von LOCAL auf AGGREGATOR oder zurück	Schreiben	index*		
UpdateView	Gewährt die Berechtigung zum Ändern von einigen der Details einer Ansicht	Schreiben	view*		

Von AWS Resource Explorer definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
view	`arn:${Partition}:resource-explorer-2:${Region}:${Account}:view/${ViewName}/${ViewUuid}`	aws:ResourceTag/${TagKey}
index	`arn:${Partition}:resource-explorer-2:${Region}:${Account}:index/${IndexUuid}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Resource Explorer

AWS Resource Explorer definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff über die Tag-Schlüssel, die an die Ressource angehängt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Resource Group Tagging API

Amazon Resource Group Tagging API (Servicepräfix: `tag`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Resource Group Tagging API definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeReportCreation	Beschreiben Sie den Status der Produktion StartReportCreation.	Lesen			
GetComplianceSummary	Gewährt die Berechtigung zum Abrufen einer Zusammenfassung der Ressourcen, die nicht mit ihren effektiven Tag-Richtlinien übereinstimmen	Lesen			
GetResources	Erteilt die Berechtigung zum Zurückgeben von getaggten oder zuvor markierten Ressourcen im angegebenen AWS-Region für das aufrufende Konto	Lesen			
GetTagKeys	Erteilt die Berechtigung zum Zurückgeben von Tag-Schlüsseln, die derzeit im angegebenen AWS-Region für das aufrufende Konto verwendet werden	Lesen			
GetTagValues	Gewährt die Berechtigung zum Zurückgeben von Tag-	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Werten für den angegebenen Schlüssel, der im angegebenen AWS-Region für das anrufende Konto				
StartReportCreation	Erstellen Sie einen Bericht, der alle markierten Ressourcen in Konten in Ihrer Organisation auflistet und ob jede Ressource mit der effektiven Tag-Richtlinie übereinstimmt.	Schreiben			
TagResources	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Tags zur angegebenen Ressource	Markierung			
UntagResources	Gewährt die Berechtigung zum Entfernen der angegebenen Ressourcen aus der angegebenen Gruppe	Markierung			

Von der Amazon Resource Group Tagging-API definierte Ressourcentypen

Die Amazon Resource Group Tagging-API unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf die Amazon Resource Group Tagging-API zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für Amazon Resource Group Tagging API

Resource Group Tagging besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen

Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Resource Groups

AWS Resource Groups (Servicepräfix: `resource-groups`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Resource Groups definierte Aktionen
- Von AWS Resource Groups definierte Ressourcentypen
- Bedingungsschlüssel für AWS Resource Groups

Von AWS Resource Groups definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden.

Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Associate Resource [nur Berechtigung]	Gewährt die Berechtigung, einer Anwendung eine Ressource zuzuordnen	Schreiben	group*		
CreateGroup	Gewährt die Berechtigung zum Erstellen einer Ressourcengruppe mit dem Namen, der Beschreibung und der Ressourcenabfrage, die angegeben wurden	Write		aws:RequestTag/${TagKey} aws:TagKeys	cloudformation:DescribeStacks

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteGroup	Gewährt die Berechtigung zum Löschen einer angegebenen Ressourcengruppe	Schreiben	group*		
DeleteGroupPolicy [nur Berechtigung]	Gewährt die Berechtigung zum Löschen einer ressourcenbasierten Richtlinie für die angegebene Gruppe	Schreiben	group*		
DisassociateResource [nur Berechtigung]	Gewährt die Berechtigung, das Mapping einer Ressource zu einer Anwendung zu trennen	Schreiben	group*		
GetAccountSettings	Gewährt die Berechtigung zum Abrufen des aktuellen Status der optionalen Funktionen in Ressourcengruppen	Lesen			
GetGroup	Gewährt die Berechtigung zum Abrufen von Informationen zu einer angegebenen Ressourcengruppe	Read	group*		
GetGroupConfiguration	Gewährt die Berechtigung zum Abrufen der Servicekonfiguration, die der angegebenen Ressourcengruppe zugeordnet ist	Lesen	group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetGroupPolicy [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen einer ressourcenbasierten Richtlinie für die angegebene Gruppe	Lesen	group*		
GetGroupQuery	Gewährt die Berechtigung zum Abrufen der Abfrage, die der angegebenen Ressourcengruppe zugeordnet ist	Read	group*		
GetTags	Gewährt die Berechtigung zum Abrufen der Tags, die der angegebenen Ressourcengruppe zugeordnet sind	Read	group*		
GroupResources	Gewährt die Berechtigung zum Hinzufügen der angegebenen Ressourcen zur angegebenen Gruppe	Write	group*		
ListGroupResources	Gewährt die Berechtigung zum Auflisten der Ressourcen, die Mitglieder der angegebenen Ressourcengruppe sind	List	group*		cloudformation:DescribeStacks cloudformation:ListStackResources tag:GetResources

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListGroups	Gewährt die Berechtigung zum Auflisten aller Resource Groups in Ihrem Konto	Auflisten			
ListResourceTypes [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten unterstützter Ressourcentypen	Auflisten			
PutGroupConfiguration	Gewährt die Berechtigung zum Setzen der Servicekonfiguration, die der angegebenen Ressourcengruppe zugeordnet ist	Write	group*		
PutGroupPolicy [nur Berechtigung]	Gewährt die Berechtigung zum Hinzufügen einer ressourcenbasierten Richtlinie für die angegebene Gruppe	Schreiben	group*		
SearchResources	Gewährt die Berechtigung zum Suchen nach AWS Ressourcen, die der angegebenen Abfrage entsprechen	Auflisten			cloudformation:DescribeStacks cloudformation:ListStackResources tag:GetResources

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Tag	Gewährt die Berechtigung zum Markieren einer angegebenen Ressourcengruppe	Markieren	group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UngroupResources	Gewährt die Berechtigung zum Entfernen der angegebenen Ressourcen aus der angegebenen Gruppe	Write	group*		
Untag	Gewährt die Berechtigung zum Entfernen von Tags, die der angegebenen Ressourcengruppe zugeordnet sind	Tagging	group*		
				aws:TagKeys	
UpdateAccountSettings	Gewährt die Berechtigung zum Aktualisieren von optionalen Funktionen in Ressourcengruppen	Schreiben			
UpdateGroup	Gewährt die Berechtigung zum Aktualisieren einer angegebenen Ressourcengruppe	Write	group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateGroupQuery	Gewährt die Berechtigung zum Aktualisieren der Abfrage, die der angegebenen Ressourcengruppe zugeordnet ist	Write	group*		cloudformation:DescribeStacks

Von AWS Resource Groups definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
group	`arn:${Partition}:resource-groups:${Region}:${Account}:group/${GroupName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Resource Groups

AWS Resource Groups definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	String
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon RHEL Knowledgebase Portal

Amazon RHEL Knowledgebase Portal (Servicepräfix: `rhelkb`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon RHEL Knowledgebase Portal definierte Aktionen
- Von Amazon RHEL Knowledgebase Portal definierte Ressourcentypen
- Bedingungsschlüssel für Amazon RHEL Knowledgebase Portal

Von Amazon RHEL Knowledgebase Portal definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetRhelURL	Erteilt die Berechtigung zum Zugreifen auf das Amazon RHEL Knowledgebase Portal	Lesen			

Von Amazon RHEL Knowledgebase Portal definierte Ressourcentypen

Amazon RHEL Knowledgebase Portal unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf Amazon RHEL Knowledgebase Portal zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für Amazon RHEL Knowledgebase Portal

RHEL KB umfasst keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS RoboMaker

AWS RoboMaker (Servicepräfix: `robomaker`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS RoboMaker definierte Aktionen
- Von AWS RoboMaker definierte Ressourcentypen

- Bedingungsschlüssel für AWS RoboMaker

Von AWS RoboMaker definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchDeleteWorlds	Mindestens eine Welt in einem Batchvorgang löschen	Write			
BatchDescribeSimulationJob	Mehrere Simulationsaufträge beschreiben	Read			
CancelDeploymentJob	Einen Bereitstellungsauftrag abbrechen	Write	deploymentJob*		
CancelSimulationJob	Einen Simulationsauftrag abbrechen	Write	simulationJob*		
CancelSimulationJobBatch	Abbrechen eines Simulationsauftragsbatches	Write	simulationJobBatch*		
CancelWorldExportJob	Ein Weltexportaufgabe stornieren	Write	worldExportJob*		
CancelWorldGenerationJob	Eine Weltgenerierungsaufgabe stornieren	Write	worldGenerationJob*		
CreateDeploymentJob	Erstellen eines Bereitstellungsauftrags	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreateFleet	Eine Bereitstellungsflotte, die eine logische Gruppe von Robotern repräsentiert, die	Write		aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	dieselbe Roboteranwendung ausführen, erstellen			aws:RequestTag/${TagKey}	
CreateRobot	Einen Roboter erstellen, der für eine Flotte registriert werden kann	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreateRobotApplication	Eine Roboteranwendung erstellen	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateRobotApplicationVersion	Einen Snapshot einer Roboteranwendung erstellen	Write	robotApplication*		s3:GetObject
CreateSimulationApplication	Eine Simulationsanwendung erstellen	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateSimulationApplicationVersion	Einen Snapshot einer Simulationsanwendung erstellen	Write	simulationApplication*		s3:GetObject

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSimulationJob	Einen Simulationsauftrag erstellen	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreateWorldExportJob	Ein Weltexportaufgabe erstellen	Write	world*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateWorldGenerationJob	Weltgenerationsaufgabe erstellen	Write	worldTemplate*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateWorldTemplate	Eine Weltvorlage erstellen	Write		aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteFleet	Eine Bereitstellungsgruppe löschen	Write	deploymentFleet*		
DeleteRobot	Einen Roboter löschen	Write	robot*		
DeleteRobotApplication	Eine Roboteranwendung löschen	Write	robotApplication*		
DeleteSimulationApplication	Eine Simulationsanwendung löschen	Write	simulationApplication*		
DeleteWorldTemplate	Eine Weltvorlage löschen	Write	worldTemplate*		
DeregisterRobot	Die Registrierung eines Roboters bei einer Flotte aufheben	Write	deploymentFleet* robot*		
DescribeDeploymentJob	Einen Bereitstellungsauftrag beschreiben	Read	deploymentJob*		
DescribeFleet	Eine Bereitstellungsflotte beschreiben	Read	deploymentFleet*		
DescribeRobot	Einen Roboter beschreiben	Read	robot*		
DescribeRobotApplication	Eine Roboteranwendung beschreiben	Read	robotApplication*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeSimulationApplication	Eine Simulationsanwendung beschreiben	Read	simulationApplication*		
DescribeSimulationJob	Einen Simulationsauftrag beschreiben	Read	simulationJob*		
DescribeSimulationJobBatch	Beschreiben eines Simulationsauftragsbatches	Read	simulationJobBatch*		
DescribeWorld	Eine Welt beschreiben	Read	world*		
DescribeWorldExportJob	Eine Weltexportaufgabe beschreiben	Read	worldExportJob*		
DescribeWorldGenerationJob	Weltgenerationsaufgabe beschreiben	Read	worldGenerationJob*		
DescribeWorldTemplate	Eine Weltvorlage beschreiben	Read	worldTemplate*		
GetWorldTemplateBody	Text einer Weltvorlage abrufen	Read	worldTemplate*		
ListDeploymentJobs	Bereitstellungsaufträge auflisten	List			
ListFleets	Flotten auflisten	List			
ListRobotApplications	Roboteranwendungen auflisten	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListRobots	Roboter auflisten	List			
ListSimulationApplications	Simulationsanwendungen auflisten	List			
ListSimulationJobBatches	Auflisten von Simulationsauftragsbatches	List			
ListSimulationJobs	Simulationsaufträge auflisten	List			
ListSupportedAvailabilityZones [nur Berechtigung]	Führt unterstützte Availability Zones auf	Auflisten			
ListTagsForResource	Auflisten von Tags für eine RoboMaker-Ressource	Auflisten	deploymentFleet		
			deploymentJob		
			robot		
			robotApplication		
			simulationApplication		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			simulationJob		
			simulationJobBatch		
			world		
			worldExportJob		
			worldGenerationJob		
			worldTemplate		
ListWorldExportJobs	Weltexportaufgaben aufführen	List			
ListWorldGenerationJobs	Weltgenerationsaufgaben auflisten	List			
ListWorldTemplates	Weltvorlagen aufführen	List			
ListWorlds	Welten auflisten	List			
RegisterRobot	Einen Roboter bei einer Flotte registrieren	Write	deploymentFleet*		
			robot*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RestartSimulationJob	Einen laufenden Simulationsauftrag neu starten	Write	simulationJob*		
StartSimulationJobBatch	Erstellen eines Simulationsauftragsbatches	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
SyncDeploymentJob	Stellt sicher, dass die zuletzt bereitgestellte Roboteranwendung für alle Roboter in der Flotte bereitgestellt wird.	Write	deploymentFleet*		iam:CreateServiceLinkedRole
TagResource	Tags einer RoboMaker-Ressource hinzufügen	Markierung	deploymentFleet		
			deploymentJob		
			robot		
			robotApplication		
			simulationApplication		
			simulationJob		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			simulationJobBatch		
			world		
			worldExportJob		
			worldGenerationJob		
			worldTemplate		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Tags aus einer RoboMaker-Ressource entfernen	Markierung	deploymentFleet		
			deploymentJob		
			robot		
			robotApplication		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			simulationApplication		
			simulationJob		
			simulationJobBatch		
			world		
			worldExportJob		
			worldGenerationJob		
			worldTemplate		
				aws:TagKeys	
UpdateRobotApplication	Eine Roboteranwendung aktualisieren	Write	robotApplication*		
UpdateRobotDeployment [nur Berechtigung]	Bereitstellungsstatus für einen einzelnen Roboter melden	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateSimulationApplication	Eine Simulationsanwendung aktualisieren	Write	simulationApplication*		
UpdateWorldTemplate	Einer Weltvorlage aktualisieren	Write	worldTemplate*		

Von AWS RoboMaker definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
robotApplication	`arn:${Partition}:robomaker:${Region}:${Account}:robot-application/${ApplicationName}/${CreatedOnEpoch}`	aws:ResourceTag/${TagKey}
simulationApplication	`arn:${Partition}:robomaker:${Region}:${Account}:simulation-application/${ApplicationName}/${CreatedOnEpoch}`	aws:ResourceTag/${TagKey}
simulationJob	`arn:${Partition}:robomaker:${Region}:${Account}:simulation-job/${SimulationJobId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
simulationJobBatch	arn:${Partition}:robomaker:${Region}:${Account}:simulation-job-batch/${SimulationJobBatchId}	aws:ResourceTag/${TagKey}
deploymentJob	arn:${Partition}:robomaker:${Region}:${Account}:deployment-job/${DeploymentJobId}	aws:ResourceTag/${TagKey}
robot	arn:${Partition}:robomaker:${Region}:${Account}:robot/${RobotName}/${CreatedOnEpoch}	aws:ResourceTag/${TagKey}
deploymentFleet	arn:${Partition}:robomaker:${Region}:${Account}:deployment-fleet/${FleetName}/${CreatedOnEpoch}	aws:ResourceTag/${TagKey}
worldGenerationJob	arn:${Partition}:robomaker:${Region}:${Account}:world-generation-job/${WorldGenerationJobId}	aws:ResourceTag/${TagKey}
worldExportJob	arn:${Partition}:robomaker:${Region}:${Account}:world-export-job/${WorldExportJobId}	aws:ResourceTag/${TagKey}
worldTemplate	arn:${Partition}:robomaker:${Region}:${Account}:world-template/${WorldTemplateJobId}	aws:ResourceTag/${TagKey}
world	arn:${Partition}:robomaker:${Region}:${Account}:world/${WorldId}	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS RoboMaker

AWS RoboMaker definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die

Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüsseln, die in der Anforderung übergeben werden.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Route 53

Amazon Route 53 (Servicepräfix: `route53`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Route 53 definierte Aktionen
- Von Amazon Route 53 definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Route 53

Von Amazon Route 53 definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ActivateKeySigningKey	Gewährt die Erlaubnis, einen Schlüsselsignaturschlüssel zu aktivieren, damit er für die Signierung durch DNSSEC verwendet werden kann	Write	hostedzone*		
AssociateVPCWithHostedZone	Gewährt die Berechtigung zum Zuordnen einer zusätzlichen Amazon-VPC zu einer privat gehosteten Zone	Schreiben	hostedzone		ec2:DescribeVpcs
ChangeCidrCollection	Gewährt die Berechtigung zum Erstellen oder Löschen von CIDR-Blöcken in einer CIDR-Sammlung	Schreiben	cidrcollection*		
ChangeResourceRecordSets	Gewährt die Berechtigung zum Erstellen, Aktualisieren oder Löschen eines Datensatzes, der autoritative DNS-Informationen für einen angegebenen Domain- oder Subdomain-Namen enthält	Write	hostedzone*		
				route53:ChangeResourceRecordSetsNormalizedRecordNames route53:ChangeResourceRecordSetsRecordTypes	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				route53:ChangeResourceRecordSetsActions	
ChangeTagsForResource	Gewährt die Berechtigung zum Hinzufügen, Bearbeiten oder Löschen von Tags für eine Zustandsprüfung oder eine gehostete Zone	Markierung	healthcheck*		
			hostedzone*		
CreateCidrCollection	Gewährt die Berechtigung zum Erstellen einer neuen CIDR-Sammlung	Schreiben			
CreateHealthCheck	Gewährt die Berechtigung zum Erstellen einer neuen Zustandsprüfung, die Zustand und Leistung von Webanwendungen, Web-Servern und anderen Ressourcen überwacht	Write			
CreateHostedZone	Gewährt die Berechtigung zum Erstellen einer öffentlich gehosteten Zone, mit der Sie festlegen können, wie das Domain Name System (DNS) Datenverkehr im Internet für eine Domain (z. B. example.com) und deren Subdomains weiterleitet	Write			ec2:DescribeVpcs

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateKeySigningKey	Gewährt die Berechtigung zum Erstellen eines neuen Schlüsselsignaturschlüssels, der einer gehosteten Zone zugeordnet ist	Write	hostedzone*		
CreateQueryLoggingConfig	Gewährt die Berechtigung zum Erstellen einer Konfiguration für die DNS-Abfrageprotokollierung	Write	hostedzone*		
CreateReusableDelegationSet	Gewährt die Berechtigung zum Erstellen eines Delegationssatzes (Gruppe von vier Namensservern), der in mehreren gehosteten Zonen wiederverwendet werden kann	Write			
CreateTrafficPolicy	Gewährt die Berechtigung zum Erstellen einer Datenverkehrsrichtlinie, mit der Sie mehrere DNS-Datensätze für einen Domain-Namen (z. B. example.com) oder Subdomain-Namen (z. B. www.example.com) erstellen können	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTrafficPolicyInstance	Gewährt die Berechtigung zum Erstellen von Datensätzen in einer angegebenen gehosteten Zone basierend auf den Einstellungen in der angegebenen Datenverkehrsrichtlinienversion	Write	hostedzone* trafficpolicy*		
CreateTrafficPolicyVersion	Gewährt die Berechtigung zum Erstellen einer neuen Version einer vorhandenen Datenverkehrsrichtlinie	Write	trafficpolicy*		
CreateVPCAssociationAuthorization	Gewährt die Berechtigung, das AWS-Konto, das eine bestimmte VPC erstellt hat, zum Erstellen einer AssociateVPCWithHostedZone-Anforderung zu autorisieren, die die VPC einer angegebenen, von einem anderen Konto erstellten gehosteten Zone zuordnet	Write	hostedzone*		
DeactivateKeySigningKey	Gewährt die Erlaubnis, einen Schlüsselsignaturschlüssel zu deaktivieren, damit er nicht für die Signierung durch DNSSEC verwendet wird	Schreiben	hostedzone*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteCidrCollection	Gewährt die Berechtigung zum Löschen einer CIDR-Sammlung	Schreiben	cidrcollection*		
DeleteHealthCheck	Gewährt die Berechtigung zum Löschen einer Zustandsprüfung	Write	healthcheck*		
DeleteHostedZone	Gewährt die Berechtigung zum Löschen einer gehosteten Zone	Write	hostedzone*		
DeleteKeySigningKey	Gewährt die Berechtigung zum Löschen eines Schlüsselsignaturschlüssels	Write	hostedzone*		
DeleteQueryLoggingConfig	Gewährt die Berechtigung zum Löschen einer Konfiguration für die DNS-Abfrageprotokollierung	Write	queryloggingconfig*		
DeleteReusableDelegationSet	Gewährt die Berechtigung zum Löschen eines wiederverwendbaren Delegationssatzes	Write	delegationset*		
DeleteTrafficPolicy	Gewährt die Berechtigung zum Löschen einer Datenverkehrsrichtlinie	Write	trafficpolicy*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteTrafficPolicyInstance	Gewährt die Berechtigung zum Löschen einer Datenverkehrsrichtlinien-Instance und aller Datensätze, die Route 53 beim Erstellen der Instance erstellt hat	Write	trafficpolicyinstance*		
DeleteVPCAssociationAuthorization	Gewährt die Berechtigung zum Entfernen der Autorisierung, eine Amazon Virtual Private Cloud einer privaten gehosteten Amazon Route 53-Zone zuzuordnen	Write	hostedzone*		
DisableHostedZoneDNSSEC	Gewährt die Berechtigung zum Deaktivieren der DNSSEC-Signierung in einer bestimmten gehosteten Zone	Write	hostedzone*		
DisassociateVPCFromHostedZone	Gewährt die Berechtigung zum Aufheben der Mapping einer Amazon Virtual Private Cloud zu einer privaten gehosteten Amazon Route 53-Zone	Write	hostedzone		ec2:DescribeVpcs
EnableHostedZoneDNSSEC	Gewährt die Berechtigung zum Aktivieren der DNSSEC-Signierung in einer bestimmten gehosteten Zone	Write	hostedzone*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAccountLimit	Gewährt die Berechtigung zum Abrufen des angegebenen Grenzwert für das aktuelle Konto, z. B. der maximalen Anzahl von Zustandsprüfungen, die Sie unter Verwendung des Kontos erstellen können	Read			
GetChange	Gewährt die Berechtigung zum Abrufen des aktuellen Status einer Anforderung zum Erstellen, Aktualisieren oder Löschen einzelner oder mehrerer Datensätze	List	change*		
GetCheckerIpRanges	Gewährt die Berechtigung zum Abrufen einer Liste der IP-Bereiche, die von Route 53-Zustandsprüfungen verwendet werden, um den Zustand von Ressourcen zu prüfen	List			
GetDNSSEC	Gewährt die Berechtigung zum Abrufen von Informationen über DNSSEC für eine bestimmte gehostete Zone, einschließlich der Schlüsselsignierschlüssel in der gehosteten Zone	Read	hostedzone*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetGeoLocation	Gewährt die Berechtigung zum Abrufen der Information, ob ein angegebener geografischer Ort für Route 53-Geolokationsdatensätze unterstützt wird	List			
GetHealthCheck	Gewährt die Berechtigung zum Abrufen von Informationen zu einer angegebenen Zustandsprüfung	Read	healthcheck*		
GetHealthCheckCount	Gewährt die Berechtigung zum Abrufen der Anzahl von Zustandsprüfungen, die dem aktuellen AWS-Konto zugeordnet sind	List			
GetHealthCheckLastFailureReason	Gewährt die Berechtigung zum Abrufen des Grunds für das letzte Fehlschlagen der angegebenen Zustandsprüfung	List	healthcheck*		
GetHealthCheckStatus	Gewährt die Berechtigung zum Abrufen des Status einer angegebenen Zustandsprüfung	List	healthcheck*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetHostedZone	Gewährt die Berechtigung zum Abrufen von Informationen zur angegebenen gehosteten Zone (einschließlich der vier Namensserver, die Route 53 der gehosteten Zone zugeordnet hat)	List	hostedzone*		
GetHostedZoneCount	Gewährt die Berechtigung zum Abrufen der Anzahl gehosteter Zonen, die dem aktuellen AWS-Konto zugeordnet sind	List			
GetHostedZoneLimit	Gewährt die Berechtigung zum Abrufen des angegebenen Limits für die angegebene gehostete Zone	Read	hostedzone*		
GetQueryLoggingConfig	Gewährt die Berechtigung zum Abrufen von Informationen zur angegebenen Konfiguration für die DNS-Abfrageprotokollierung	Read	queryloggingconfig*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetReusableDelegationSet	Gewährt die Berechtigung zum Abrufen von Informationen zum angegebenen wiederverwendbaren Delegationssatz (einschließlich der vier Namensserver, die dem Delegationssatz zugeordnet sind)	List	delegationset*		
GetReusableDelegationSetLimit	Gewährt die Berechtigung zum Abrufen der maximalen Anzahl gehosteter Zonen, die Sie dem angegebenen wiederverwendbaren Delegationssatz zuordnen können	Read	delegationset*		
GetTrafficPolicy	Gewährt die Berechtigung zum Abrufen von Informationen zu einer angegebenen Datenverkehrsrichtlinienversion	Read	trafficpolicy*		
GetTrafficPolicyInstance	Gewährt die Berechtigung zum Abrufen von Informationen zu einer angegebenen Datenverkehrsrichtlinien-Instance	Read	trafficpolicyinstance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetTrafficPolicyInstanceCount	Gewährt die Berechtigung zum Abrufen der Anzahl von Datenverkehrsrichtlinien-Instances, die dem aktuellen AWS-Konto zugeordnet sind	Lesen			
ListCidrBlocks	Gewährt die Berechtigung zum Abrufen einer Liste der CIDR-Blöcke innerhalb einer bestimmten CIDR-Sammlung	Auflisten	cidrcollection*		
ListCidrCollections	Gewährt die Berechtigung zum Abrufen einer Liste der CIDR-Sammlungen, die dem aktuellen AWS-Konto zugeordnet sind	Auflisten			
ListCidrLocations	Gewährt die Berechtigung zum Abrufen einer Liste der CIDR-Speicherorte, die zu einer bestimmten CIDR-Sammlung gehören	Auflisten	cidrcollection*		
ListGeoLocations	Gewährt die Berechtigung zum Abrufen einer Liste geografischer Orte, die von Route 53 für die Geolokation unterstützt werden	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListHealthChecks	Gewährt die Berechtigung zum Abrufen einer Liste der Zustandsprüfungen, die dem aktuellen AWS-Konto zugeordnet sind	Lesen			
ListHostedZones	Gewährt die Berechtigung zum Abrufen einer Liste öffentlich und privat gehosteter Zonen, die dem aktuellen AWS-Konto zugeordnet sind	List			
ListHostedZonesByName	Gewährt die Berechtigung zum Abrufen einer Liste der gehosteten Zonen in lexikografischer Reihenfolge. Gehostete Zonen werden nach Name sortiert (mit den Namensbestandteilen in umgekehrter Reihenfolge, z. B. com.example.www)	Auflisten			
ListHostedZonesByVPC	Gewährt die Berechtigung zum Abrufen einer Liste aller privaten gehosteten Zonen, denen eine angegebene VPC zugeordnet ist	Auflisten			ec2:DescribeVpcs

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListQueryLoggingConfigs	Gewährt die Berechtigung zum Auflisten der Konfigurationen für die DNS-Abfrageprotokollierung, die dem aktuellen AWS-Konto zugeordnet sind, oder der Konfiguration, die der angegebenen gehosteten Zone zugeordnet ist	Auflisten	hostedzone		
ListResourceRecordSets	Gewährt die Berechtigung zum Auflisten der Datensätze in der angegebenen gehosteten Zone	List	hostedzone*		
ListReusableDelegationSets	Gewährt die Berechtigung zum Auflisten der wiederverwendbaren Delegationssätze, die dem aktuellen AWS-Konto zugeordnet sind	Lesen			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Zustandsprüfung oder gehostete Zone	Lesen	healthcheck		
			hostedzone		
ListTagsForResources	Gewährt die Berechtigung zum Auflisten von Tags für bis zu 10 Zustandsprüfungen oder gehostete Zonen	Lesen	healthcheck		
			hostedzone		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTrafficPolicies	Gewährt die Berechtigung zum Abrufen von Informationen zur neuesten Version aller Datenverkehrsrichtlinien, die dem aktuellen AWS-Konto zugeordnet sind. Die Richtlinien werden in der Reihenfolge der Erstellung aufgelistet	Auflisten			
ListTrafficPolicyInstances	Gewährt die Berechtigung zum Abrufen von Informationen zu Datenverkehrsrichtlinien-Instances, die Sie unter Verwendung des aktuellen AWS-Konto erstellt haben	Lesen			
ListTrafficPolicyInstancesByHostedZone	Gewährt die Berechtigung zum Abrufen von Informationen zu Datenverkehrsrichtlinien-Instances, die Sie in der angegebenen gehosteten Zone erstellt haben	List	hostedzone*		
ListTrafficPolicyInstancesByPolicy	Gewährt die Berechtigung zum Abrufen von Informationen zu Datenverkehrsrichtlinien-Instances, die Sie unter Verwendung der angegebenen Datenverkehrsrichtlinienversion erstellt haben	List	trafficpolicy*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTrafficPolicyVersions	Gewährt die Berechtigung zum Abrufen von Informationen zu allen Versionen der angegebenen Datenverkehrsrichtlinie	List	trafficpolicy*		
ListVPCAssociationAuthorizations	Gewährt die Berechtigung zum Abrufen einer Liste der VPCs, die von anderen Konten erstellt wurden und einer angegebenen gehosteten Zone zugeordnet werden können	List	hostedzone*		
TestDNSAnswer	Gewährt die Berechtigung zum Abrufen des Werts, den Route 53 als Antwort auf eine DNS-Abfrage für einen angegebenen Datensatznamen und -typ zurückgibt	Read			
UpdateHealthCheck	Gewährt die Berechtigung zum Aktualisieren einer Zustandsprüfung	Write	healthcheck*		
UpdateHostedZoneComment	Gewährt die Berechtigung zum Aktualisieren eines Kommentars für die angegebene gehostete Zone	Write	hostedzone*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateTrafficPolicyComment	Gewährt die Berechtigung zum Aktualisieren des Kommentars für die angegebene Datenverkehrsrichtlinienversion	Write	trafficpolicy*		
UpdateTrafficPolicyInstance	Gewährt die Berechtigung zum Aktualisieren der Datensätze in einer angegebenen gehosteten Zone, die basierend auf den Einstellungen in einer angegebenen Datenverkehrsrichtlinienversion erstellt wurde	Write	trafficpolicyinstance*		

Von Amazon Route 53 definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
cidrcollection	`arn:${Partition}:route53:::cidrcollection/${Id}`	

Ressourcentypen	ARN	Bedingungsschlüssel
change	arn:${Partition}:route53:::change/${Id}	
delegationset	arn:${Partition}:route53:::delegationset/${Id}	
healthcheck	arn:${Partition}:route53:::healthcheck/${Id}	
hostedzone	arn:${Partition}:route53:::hostedzone/${Id}	
trafficpolicy	arn:${Partition}:route53:::trafficpolicy/${Id}	
trafficpolicyinstance	arn:${Partition}:route53:::trafficpolicyinstance/${Id}	
queryloggingconfig	arn:${Partition}:route53:::queryloggingconfig/${Id}	
vpc	arn:${Partition}:ec2:${Region}:${Account}:vpc/${VpcId}	

Bedingungsschlüssel für Amazon Route 53

Amazon Route 53 definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
route53:ChangeResourceRecordSetsActions	Filtert den Zugriff durch die Änderungsaktionen CREATE, UPSERT oder DELETE in einer ChangeResourceRecordSets-Anforderung	ArrayOfString
route53:ChangeResourceRecordSetsNormalizedRecordNames	Filtert den Zugriff durch die normalisierten DNS-Datensatznamen in einer ChangeResourceRecordSets-Anforderung	ArrayOfString
route53:ChangeResourceRecordSetsRecordTypes	Filtert den Zugriff durch die DNS-Datensatztypen in einer ChangeResourceRecordSets-Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Route 53 Recovery Controller – Zonal Shift

Amazon Route 53 Application Recovery Controller – Zonal Shift (Servicepräfix: `arc-zonal-shift`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Route 53 Application Recovery Controller – Zonal Shift definierte Aktionen
- Von Amazon Route 53 Application Recovery Controller – Zonal Shift definierte Ressourcentypen
- Bedingungsschlüssel Amazon Route 53 Application Recovery Controller – Zonal Shift

Von Amazon Route 53 Application Recovery Controller – Zonal Shift definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelZonalShift	Gewährt die Berechtigung zum Abbrechen einer aktiven Zonal Shift	Schreiben	ALB*		
			NLB*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreatePracticeRunConfiguration	Gewährt die Berechtigung zum Erstellen einer Praxislauf-Konfiguration	Schreiben	ALB*		cloudwatch:DescribeAlarms iam:CreateServiceLinkedRole
			NLB*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				elasticloadbalancing:ResourceTag/${TagKey}	
DeletePracticeRunConfiguration	Gewährt die Berechtigung zum Löschen einer Praxislauf-Konfiguration	Schreiben	ALB*		
			NLB*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
GetManagedResource	Gewährt die Berechtigung zum Abrufen von Informationen zu einer verwalteten Ressource	Lesen	ALB*		
			NLB*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ListAutoshifts	Gewährt die Berechtigung zum Auflisten von aktiven und abgeschlossenen Autoshifts	Auflisten			
ListManagedResources	Gewährt die Berechtigung zum Auflisten von verwaltete Ressourcen	Auflisten			
ListZonalShifts	Gewährt die Berechtigung zum Auflisten von Zonal Shifts	Auflisten			
StartZonalShift	Gewährt die Berechtigung zum Starten von Zonal Shift	Schreiben	ALB* NLB*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
UpdatePracticeRunConfiguration	Gewährt die Berechtigung zum Aktualisieren einer Praxislauf–Konfiguration	Schreiben	ALB*		cloudwatch:DescribeAlarms iam:CreateServiceLinkedRole
			NLB*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateZonalAutoshiftConfiguration	Gewährt die Berechtigung zum Aktualisieren eines zonalen Autoshift-Status	Schreiben	ALB*		
			NLB*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
UpdateZonalShift	Gewährt die Berechtigung zum Aktualisieren eines bestehenden Zonal Shifts	Schreiben	ALB*		
			NLB*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Von Amazon Route 53 Application Recovery Controller – Zonal Shift definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
ALB	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}`	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
NLB	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/net/${LoadBalancerName}/${LoadBalancerId}`	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

Bedingungsschlüssel Amazon Route 53 Application Recovery Controller – Zonal Shift

Amazon Route 53 Recovery Controller - Zonal Shift definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der verwalteten Ressource zugeordnet sind.	String
elasticloadbalancing:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der verwalteten Ressource zugeordnet sind.	String

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Route 53 Domains

Amazon Route 53 Domains (Servicepräfix: `route53domains`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Route 53 Domains definierte Aktionen
- Von Amazon Route 53 Domains definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Route 53 Domains

Von Amazon Route 53 Domains definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen.

Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptDomainTransferFromAnotherAwsAccount	Gewährt die Erlaubnis, den Transfer einer Domain von einem anderen AWS-Konto auf das aktuelle AWS-Konto zu akzeptieren	Schreiben			
AssociateDelegationSignerToDomain	Gewährt die Berechtigung zum Aufheben der Zuordnung eines neuen Delegierungssignierers zu einer Domain	Schreiben			
CancelDomainTransferToAnotherAwsAccount	Gewährt die Erlaubnis, den Transfer einer Domain vom aktuellen AWS-Konto auf ein anderes AWS-Konto abzubrechen	Write			
CheckDomainAvailability	Gewährt die Berechtigung zum Überprüfen der Verfügbarkeit von einem Domain-Namen	Read			
CheckDomainTransferability	Gewährt die Erlaubnis zu prüfen, ob ein Domainname auf Amazon Route 53 übertragen werden kann	Lesen			
DeleteDomain	Gewährt die Berechtigung zum Löschen von Domains	Schreiben			
DeleteTagsForDomain	Gewährt die Berechtigung zum Löschen der angegebenen Tags für eine Domain	Markieren			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisableDomainAutoRenew	Gewährt die Berechtigung zum Konfigurieren von Amazon Route 53 zur automatischen Verlängerung der angegebenen Domain, bevor die Domain-Registrierung abläuft	Write			
DisableDomainTransferLock	Gewährt die Berechtigung zum Entfernen der Übertragungssperre auf der Domain (genauer gesagt, den Status clientTransferProhibited), um Domain-Übertragungen zu erlauben	Schreiben			
DisassociateDelegationSignerFromDomain	Gewährt die Berechtigung zum Trennen eines vorhandenen Delegierungssignierers von einer Domain	Schreiben			
EnableDomainAutoRenew	Gewährt die Berechtigung zum Konfigurieren von Amazon Route 53 zur automatischen Verlängerung der angegebenen Domain, bevor die Domain-Registrierung abläuft	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
EnableDomainTransferLock	Gewährt die Berechtigung zum Festlegen der Übertragungssperre auf der Domain (genauer gesagt, den Status clientTransferProhibited), um Domain-Übertragungen zu erlauben	Schreiben			
GetContactReachabilityStatus	Gewährt die Berechtigung zum Abrufen von Informationen darüber, ob der Registrierende auf Operationen geantwortet hat, für die eine Bestätigung der Gültigkeit der E-Mail-Adresse des Registrierenden erforderlich ist, z. B. das Registrieren einer neuen Domain	Lesen			
GetDomainDetail	Gewährt die Berechtigung zum Abrufen detaillierter Informationen zu einer Domain	Read			
GetDomainSuggestions	Gewährt die Berechtigung zum Abrufen einer Liste der vorgeschlagenen Domain-Namen mit einer Zeichenfolge zurück, die entweder ein Domain-Name oder einfach ein Wort oder ein Satz (ohne Leerzeichen) sein kann	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetOperationDetail	Gewährt die Berechtigung zum Abrufen des aktuellen Status einer Produktion, die nicht abgeschlossen ist	Read			
ListDomains	Gewährt die Berechtigung zum Auflisten aller Domain-Namen, die bei Amazon Route 53 für das aktuelle AWS-Konto registriert sind	List			
ListOperations	Gewährt die Berechtigung zum Auflisten der IDs von Produktionen, die noch nicht abgeschlossen sind	Auflisten			
ListPrices	Gewährt die Berechtigung zum Auflisten der Preise für TLDs	Auflisten			
ListTagsForDomain	Gewährt die Berechtigung zum Auflisten aller Tags, die der angegebenen Domain zugeordnet sind	Lesen			
PushDomain	Gewährt die Berechtigung zum Ändern des IPS-Tag der.uk-Domain, um einen Übertragungsprozess von Route 53 zu einem anderen Registrar einzuleiten	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RegisterDomain	Gewährt die Berechtigung zum Registrieren von Domains	Write			
RejectDomainTransferFromAnotherAwsAccount	Gewährt die Erlaubnis, den Transfer einer Domain von einem anderen AWS-Konto auf das aktuelle AWS-Konto abzulehnen	Write			
RenewDomain	Gewährt die Berechtigung zur Verlängerung von Domains für die angegebene Anzahl von Jahren	Schreiben			
ResendContactReachabilityEmail	Gewährt die Berechtigung, die Bestätigungs-E-Mail erneut an die aktuelle E-Mail-Adresse des Registrierenden zu senden, wenn Operationen die Bestätigung der Gültigkeit der E-Mail-Adresse des Registrierenden erfordern, z. B. das Registrieren einer neuen Domain	Schreiben			
ResendOperationAuthorization	Gewährt die Berechtigung, die Betriebsgenehmigung erneut zu senden	Schreiben			
RetrieveDomainAuthCode	Gewährt die Berechtigung zum Abrufen des AuthCode für die Domain	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TransferDomain	Gewährt die Berechtigung zum Übertragen einer Domain von einem anderen Registrar an Amazon Route 53	Write			
TransferDomainToAnotherAwsAccount	Gewährt die Erlaubnis, eine Domain vom aktuellen AWS-Konto auf ein anderes AWS-Konto zu übertragen	Write			
UpdateDomainContact	Gewährt die Berechtigung zum Aktualisieren der Kontaktinformationen für eine Domain	Write			
UpdateDomainContactPrivacy	Gewährt die Berechtigung zum Aktualisieren der Kontaktdatenschutzeinstellungen der Domain	Write			
UpdateDomainNameservers	Gewährt die Berechtigung zum Ersetzen des aktuellen Satzes von Namenservern für eine Domain mit dem angegebenen Satz von Namenservern	Write			
UpdateTagsForDomain	Gewährt die Berechtigung zum Hinzufügen oder Aktualisieren von Tags für eine angegebene Domain	Markieren			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ViewBilling	Gewährt die Berechtigung zum Abrufen aller domain-bezogenen Datensätze für die Fakturierung im Zusammenhang mit dem aktuellen AWS-Konto für einen bestimmten Zeitraum	Read			

Von Amazon Route 53 Domains definierte Ressourcentypen

Amazon Route 53 Domains unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf Amazon Route 53 Domains zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für Amazon Route 53 Domains

Route 53 Domains umfasst keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Route 53 53-Profile ermöglichen die gemeinsame Nutzung von DNS-Einstellungen mit VPCs

Amazon Route 53 Profiles ermöglicht die gemeinsame Nutzung von DNS-Einstellungen mit VPCs (Service-Präfix:`route53profiles`) und bietet die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.

- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Durch Amazon Route 53 Profiles definierte Aktionen ermöglichen die gemeinsame Nutzung von DNS-Einstellungen mit VPCs
- Durch Amazon Route 53 Profiles definierte Ressourcentypen ermöglichen die gemeinsame Nutzung von DNS-Einstellungen mit VPCs
- Bedingungsschlüssel für Amazon Route 53 53-Profile ermöglichen die gemeinsame Nutzung von DNS-Einstellungen mit VPCs

Durch Amazon Route 53 Profiles definierte Aktionen ermöglichen die gemeinsame Nutzung von DNS-Einstellungen mit VPCs

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateProfile	Erteilt die Erlaubnis, der Kunden-VPC ein Profil zuzuordnen	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeVpcs
AssociateResourceToProfile	Erteilt die Berechtigung, eine Ressource, z. B. eine DNS-Firewall-Regelgruppe, eine privat gehostete Zone, eine Resolver-Regel usw., einem bestimmten Profil zuzuordnen	Schreiben			
CreateProfile	Erteilt die Berechtigung zum Erstellen einer neuen Profilressource	Schreiben		aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
DeleteProfile	Erteilt die Berechtigung zum Löschen eines Profils, das durch den ProfileId	Schreiben			
DisassociateProfile	Erteilt die Berechtigung, eine Verknüpfung zwischen einer Kunden-VPC und dem angegebenen Profil zu löschen	Schreiben			
DisassociateResourceFromProfile	Erteilt die Berechtigung zum Löschen der Zuordnung zwischen der Ressource, z. B. einer DNS-Firewall-Regelgruppe, einer privat gehosteten Zone, einer Resolver-Regel usw., und dem angegebenen Profil	Schreiben			
GetProfile	Erteilt die Berechtigung zum Abrufen eines Profils	Lesen			
GetProfileAssociation	Erteilt einer durch die Profilzuordnungs-ID angegebenen VPC-Zuordnung die Erlaubnis, ein Profil abzurufen	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetProfileResourceAssociation	Erteilt die Berechtigung zum Abrufen einer Profilressourcenverknüpfung auf der Grundlage von ProfileResourceAssociationId	Lesen			
ListProfileAssociations	Erteilt die Berechtigung, alle VPCs aufzulisten, denen das angegebene Profil zugeordnet ist	Auflisten			
ListProfileResourceAssociations	Erteilt die Berechtigung, alle Verknüpfungen zwischen den Ressourcen aufzulisten, z. B. DNS-Firewall-Regelgruppen, privat gehostete Zonen, Resolver-Regeln usw. für die angegebene Profil-ID	Auflisten			
ListProfiles	Erteilt die Berechtigung, alle Profile aufzulisten, die vom Kunden erstellt und für ihn freigegeben wurden	Auflisten			
ListTagsForResource	Erteilt die Berechtigung, alle mit der Ressource verknüpften Tags aufzulisten	Auflisten			
TagResource	Erteilt die Berechtigung, der angegebenen Ressource ein Tag hinzuzufügen	Tagging	profile		
			profile-association		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Erteilt die Erlaubnis, ein Tag aus der angegebenen Ressource zu löschen	Tagging	profile		
			profile-association		
				aws:TagKeys	
UpdateProfileResourceAssociation	Erteilt die Berechtigung, den Namen der Profilressourcenverknüpfung oder die Ressourceneigenschaften oder beides zu aktualisieren. Wenn sowohl der Name als auch die Ressourceneigenschaften Null sind, gibt die API die bestehende Profilressourcenzuordnung zurück	Schreiben			

Durch Amazon Route 53 Profiles definierte Ressourcentypen ermöglichen die gemeinsame Nutzung von DNS-Einstellungen mit VPCs

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der

Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
profile	`arn:${Partition}:route53profiles:${Region}:${Account}:profile/${ResourceId}`	aws:ResourceTag/${TagKey}
profile-association	`arn:${Partition}:route53profiles:${Region}:${Account}:profile-association/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Route 53 53-Profile ermöglichen die gemeinsame Nutzung von DNS-Einstellungen mit VPCs

Amazon Route 53 Profiles ermöglicht die gemeinsame Nutzung von DNS-Einstellungen mit VPCs und definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüsselwertpaaren, die der Ressource angefügt sind	String

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Route 53 Recovery Cluster

Amazon Route 53 Recovery Cluster (Servicepräfix: `route53-recovery-cluster`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Route 53 Recovery Cluster definierte Aktionen
- Von Amazon Route 53 Recovery Cluster definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Route 53 Recovery Cluster

Von Amazon Route 53 Recovery Cluster definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetRoutingControlState	Gewährt die Berechtigung zum Abrufen eines Routing-Kontrollstatus	Lesen	routingcontrol*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListRoutingControls	Gewährt die Berechtigung zum Auflisten von Routenkontrollen	Lesen			
UpdateRoutingControlState	Gewährt die Berechtigung zum Aktualisieren eines Routing-Kontrollstatus	Schreiben	routingcontrol*		
				route53-recovery-cluster:AllowSafetyRulesOverrides	
UpdateRoutingControlStates	Gewährt die Berechtigung zum Aktualisieren eines Routing-Kontrollstatus-Batch	Schreiben	routingcontrol*		
				route53-recovery-cluster:AllowSafetyRulesOverrides	

Von Amazon Route 53 Recovery Cluster definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
routingcontrol	`arn:${Partition}:route53-recovery-control::${Account}:controlpanel/${ControlPanelId}/routingcontrol/${RoutingControlId}`	

Bedingungsschlüssel für Amazon Route 53 Recovery Cluster

Amazon Route 53 Recovery Cluster definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
route53-recovery-cluster:AllowSafetyRulesOverrides	Außer Kraft setzen von Sicherheitsregeln, um Routing-Steuerstatusaktualisierungen zu erlauben	Bool

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Route 53 Recovery Controls

Amazon Route 53 Recovery Controls (Servicepräfix: `route53-recovery-control-config`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Route 53 Recovery Controls definierte Aktionen
- Von Amazon Route 53 Recovery Controls definierte Resssourcentypen
- Bedingungsschlüssel für Amazon Route 53 Recovery Controls

Von Amazon Route 53 Recovery Controls definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCluster	Gewährt die Berechtigung zum Erstellen eines Clusters	Schreiben	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateControlPanel	Gewährt die Berechtigung zum Erstellen einer Systemsteuerung	Schreiben	controlpanel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRoutingControl	Gewährt die Berechtigung zum Erstellen einer neuen Routenkontrolle	Schreiben	routingcontrol*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSafetyRule	Gewährt die Berechtigung zum Erstellen einer Sicherheitsregel	Schreiben	safetyrule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCluster	Gewährt die Berechtigung zum Löschen eines Clusters	Schreiben	cluster*		
DeleteControlPanel	Gewährt die Berechtigung zum Löschen einer Systemsteuerung	Schreiben	controlpanel*		
DeleteRoutingControl	Gewährt die Berechtigung zum Löschen einer Routenkontrolle	Write	routingcontrol*		
DeleteSafetyRule	Gewährt die Berechtigung zum Löschen einer Sicherheitsregel	Write	safetyrule*		
DescribeCluster	Gewährt die Berechtigung zum Beschreiben eines Clusters	Read	cluster*		
DescribeControlPanel	Gewährt die Berechtigung zum Beschreiben einer Systemsteuerung	Read	controlpanel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeRoutingControl	Gewährt die Berechtigung zum Beschreiben einer Routenkontrolle	Read	routingcontrol*		
DescribeRoutingControlByName	Gewährt die Berechtigung zum Beschreiben einer Routenkontrolle	Read	routingcontrol*		
DescribeSafetyRule	Gewährt die Berechtigung zum Beschreiben einer Sicherheitsregel	Lesen	safetyrule*		
GetResourcePolicy	Gewährt die Berechtigung zum Abrufen der Ressourcenrichtlinie eines Clusters	Lesen	cluster*		
ListAssociatedRoute53HealthChecks	Gewährt die Berechtigung zum Auflisten verknüpfter Route 53-Zustandsprüfungen	Auflisten			
ListClusters	Gewährt die Berechtigung zum Auflisten von Clustern	Lesen			
ListControlPanels	Gewährt die Berechtigung zum Auflisten von Systemsteuerungen	Read			
ListRoutingControls	Gewährt die Berechtigung zum Auflisten von Routenkontrollen	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListSafetyRules	Gewährt die Berechtigung zum Auflisten von Sicherheitsregeln	Lesen	controlpanel*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen			
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markierung	cluster		
			controlpanel		
			safetyrule		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Ressource	Markierung	cluster		
			controlpanel		
			safetyrule		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateControlPanel	Gewährt die Berechtigung zum Aktualisieren eines Clusters	Schreiben	controlpanel*		
UpdateRoutingControl	Gewährt die Berechtigung zum Aktualisieren der Routenkontrolle	Schreiben	routingcontrol*		
UpdateSafetyRule	Gewährt die Berechtigung zum Aktualisieren einer Sicherheitsregel	Schreiben	safetyrule*		

Von Amazon Route 53 Recovery Controls definierte Resssourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
cluster	`arn:${Partition}:route53-recovery-control::${Account}:cluster/${ResourceId}`	aws:ResourceTag/${TagKey}
controlpanel	`arn:${Partition}:route53-recovery-control::${Account}:controlpanel/${ControlPanelId}`	aws:ResourceTag/${TagKey}
routingcontrol	`arn:${Partition}:route53-recovery-control::${Account}:controlpanel/${ControlPanelId}/routingcontrol/${RoutingControlId}`	
safetyrule	`arn:${Partition}:route53-recovery-control::${Account}:controlpanel/${ControlPanelId}/safetyrule/${SafetyRuleId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Route 53 Recovery Controls

Amazon Route 53 Recovery Controls definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Schlüssel eines Tags und den Wert einer Anforderung	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Route 53 Recovery Readiness

Amazon Route 53 Recovery Readiness (Servicepräfix: `route53-recovery-readiness`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Route 53 Recovery Readiness definierte Aktionen
- Von Amazon Route 53 Recovery Readiness definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Route 53 Recovery Readiness

Von Amazon Route 53 Recovery Readiness definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCell	Gewährt die Berechtigung zum Erstellen einer neuen Zelle	Schreiben	cell*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCrossAccountAuthorization	Gewährt die Berechtigung zum Erstellen einer neuen kontenübergreifenden Autorisierung	Schreiben			
CreateReadinessCheck	Gewährt die Berechtigung zum Erstellen einer neuen Bereitschaftsprüfung	Schreiben	readinesscheck*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRecoveryGroup	Gewährt die Berechtigung zum Erstellen einer neuen Recovery-Gruppe	Schreiben	recoverygroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateResourceSet	Gewährt die Berechtigung zum Erstellen eines neuen Ressourcensatzes	Schreiben	resourceset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCell	Gewährt die Berechtigung zum Löschen einer Zelle	Schreiben	cell*		
DeleteCrossAccountAuthorization	Gewährt die Berechtigung zum Löschen einer kontenübergreifenden Autorisierung	Schreiben			
DeleteReadinessCheck	Gewährt die Berechtigung zum Löschen einer Bereitschaftsprüfung	Schreiben	readinesscheck*		
DeleteRecoveryGroup	Gewährt die Berechtigung zum Löschen einer Wiederherstellungsgruppe	Schreiben	recoverygroup*		
DeleteResourceSet	Gewährt die Berechtigung zum Löschen eines Ressourcensatzes	Schreiben	resourceset*		
GetArchitectureRecommendations	Gewährt die Berechtigung zum Abrufen von Architekturempfehlungen für eine Wiederherstellungsgruppe	Lesen	recoverygroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetCell	Gewährt Berechtigungen zum Abrufen von Informationen zu einer Zelle	Lesen	cell*		
GetCellReadinessSummary	Gewährt die Berechtigung zum Abrufen der Bereitschaftsübersicht für eine Zelle	Lesen	cell*		
GetReadinessCheck	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Bereitschaftsprüfung	Lesen	readinesscheck*		
GetReadinessCheckResourceStatus	Gewährt die Berechtigung zum Abrufen der Bereitschaftsübersicht für eine einzelne Ressource	Lesen	readinesscheck*		
GetReadinessCheckStatus	Gewährt die Berechtigung zum Abrufen des Status einer Bereitschaftsprüfung (für einen Ressourcensatz)	Lesen	readinesscheck*		
GetRecoveryGroup	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Wiederherstellungsgruppe	Lesen	recoverygroup*		
GetRecoveryGroupReadinessSummary	Gewährt die Berechtigung zum Abrufen einer Bereitschaftszusammenfassung für eine Wiederherstellungsgruppe	Lesen	recoverygroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetResourceSet	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Ressourcensatz	Lesen	resourceset*		
ListCells	Gewährt die Berechtigung zum Auflisten von Zellen	Lesen			
ListCrossAccountAuthorizations	Gewährt die Berechtigung zum Auflisten von kontenübergreifenden Berechtigungen	Lesen			
ListReadinessChecks	Gewährt die Berechtigung zum Auflisten von Bereitschaftsprüfungen	Lesen			
ListRecoveryGroups	Gewährt die Berechtigung zum Auflisten von Wiederherstellungsgruppen	Lesen			
ListResourceSets	Gewährt die Berechtigung zum Auflisten von Ressourcensätzen	Lesen			
ListRules	Gewährt die Berechtigung zum Auflisten von Bereitschaftsregeln	Read			
ListTagsForResources	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Read			
TagResource		Markieren	cell		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Gewährt die Berechtigung zum Hinzufügen eines Tags zu einer Ressource		readinesscheck		
			recoverygroup		
			resourceset		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen eines Tags von einer Ressource	Markierung	cell		
			readinesscheck		
			recoverygroup		
			resourceset		
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateCell	Gewährt die Berechtigung zum Aktualisieren einer Zelle	Schreiben	cell*		
				aws:TagKeys	
UpdateReadinessCheck	Gewährt die Berechtigung zum Aktualisieren einer Bereitschaftsprüfung	Schreiben	readinesscheck*		
				aws:TagKeys	
UpdateRecoveryGroup	Gewährt die Berechtigung zum Aktualisieren einer Wiederherstellungsgruppe	Schreiben	recoverygroup*		
				aws:TagKeys	
UpdateResourceSet	Gewährt die Berechtigung zum Aktualisieren eines Ressourcensatzes	Schreiben	resourceset*		
				aws:TagKeys	

Von Amazon Route 53 Recovery Readiness definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
readinesscheck	`arn:${Partition}:route53-recovery-readiness::${Account}:readiness-check/${ResourceId}`	aws:ResourceTag/${TagKey}
resourceset	`arn:${Partition}:route53-recovery-readiness::${Account}:resource-set/${ResourceId}`	aws:ResourceTag/${TagKey}
cell	`arn:${Partition}:route53-recovery-readiness::${Account}:cell/${ResourceId}`	aws:ResourceTag/${TagKey}
recoverygroup	`arn:${Partition}:route53-recovery-readiness::${Account}:recovery-group/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Route 53 Recovery Readiness

Amazon Route 53 Recovery Readiness definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Route 53 Resolver

Amazon Route 53 Resolver (Servicepräfix: `route53resolver`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Route 53 Resolver definierte Aktionen
- Von Amazon Route 53 Resolver definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Route 53 Resolver

Von Amazon Route 53 Resolver definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateFirewallRuleGroup	Gewährt die Berechtigung zum Verknüpfen einer Amazon VPC mit einer bestimmten Firewall-Regelgruppe	Write	firewall-rule-group-association*		ec2:DescribeVpcs
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociateResolverEndpointIpAddress	Gewährt die Berechtigung zum Verknüpfen einer angegebenen IP-Adresse mit einem Resolver-Endpunkt. Hierbei handelt es sich um eine IP-Adresse, die DNS-Abfragen an Ihr Netzwerk (ausgehend) oder Ihre VPCs (eingehend) weiterleitet.	Write	resolver-endpoint*		ec2:CreateNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets
AssociateResolverQueryLogConfig	Gewährt die Berechtigung, eine Amazon VPC mit einer angegebenen Konfiguration für die Abfrageprotokollierung zuzuordnen	Write	resolver-query-log-config*		ec2:DescribeVpcs
AssociateResolverRule	Gewährt die Berechtigung zum Verknüpfen einer	Write	resolver-rule*		ec2:DescribeVpcs

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	angegebenen Resolver-Regel mit einer bestimmten VPC				
CreateFirewallDomainList	Gewährt die Berechtigung zum Erstellen einer Firewall-Domain-Liste	Write	firewall-domain-list*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFirewallRule	Gewährt die Berechtigung zum Erstellen einer Firewall-Regel innerhalb einer Firewall-Regelgruppe.	Write	firewall-domain-list*		
			firewall-rule-group*		
CreateFirewallRuleGroup	Gewährt die Berechtigung zum Erstellen einer Firewall-Regelgruppe.	Schreiben	firewall-rule-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateOutpostResolver	Gewährt die Berechtigung zum Erstellen eines Route-53-Resolvers in Outposts	Schreiben	outpost-resolver*		outposts:GetOutpost
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateResolverEndpoint	Gewährt die Berechtigung zum Erstellen eines Resolver-Endpunkts. Es gibt zwei Arten von Resolver-Endpunkten, eingehend und ausgehend	Write	resolver-endpoint*		ec2:CreateNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateResolverQueryLogConfig	Gewährt die Berechtigung zum Erstellen einer Resolver-Abfrageprotokollierungskonfiguration, die definiert, wo Resolver DNS-Abfrageprotokolle speichern soll, die aus Ihren VPCs stammen	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateResolverRule	Gewährt die Berechtigung zum Definieren, wie bei Abfragen, die ihren Ursprung in Ihrer VPC haben, die Weiterleitung aus der VPC erfolgt	Schreiben	resolver-rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFirewallDomainList	Gewährt die Berechtigung zum Löschen einer Firewall-Domain-Liste	Write	firewall-domain-list*		
DeleteFirewallRule	Gewährt die Berechtigung zum Löschen einer Firewall-Regel innerhalb einer Firewall-Regelgruppe.	Write	firewall-domain-list*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			firewall-rule-group*		
DeleteFirewallRuleGroup	Gewährt die Berechtigung zum Löschen einer Firewall-Regelgruppe	Schreiben	firewall-rule-group*		
DeleteOutpostResolver	Gewährt die Berechtigung zum Löschen eines Route-53-Resolvers in Outposts	Schreiben	outpost-resolver*		
DeleteResolverEndpoint	Gewährt die Berechtigung zum Löschen eines Resolver-Endpunkts. Welche Auswirkungen das Löschen eines Resolver-Endpunkts hat, hängt davon ab, ob es sich um einen eingehenden oder ausgehenden Endpunkt handelt.	Write	resolver-endpoint*		ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces
DeleteResolverQueryLogConfig	Gewährt die Berechtigung zum Löschen einer Konfiguration für die Protokollierung einer Resolver-Abfrage	Write	resolver-query-log-config*		
DeleteResolverRule	Gewährt die Berechtigung zum Löschen einer Resolver-Regel	Write	resolver-rule*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateFirewallRuleGroup	Gewährt die Berechtigung zum Entfernen der Verknüpfung zwischen einer angegebenen Firewall-Regelgruppe und einer angegebenen VPC	Write	firewall-rule-group-association*		
DisassociateResolverEndpointIpAddress	Gewährt die Berechtigung zum Entfernen einer angegebenen IP-Adresse aus einem Resolver-Endpunkt. Hierbei handelt es sich um eine IP-Adresse, die DNS-Abfragen an Ihr Netzwerk (ausgehend) oder Ihre VPCs (eingehend) weiterleitet.	Write	resolver-endpoint*		ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces
DisassociateResolverQueryLogConfig	Gewährt die Berechtigung zum Aufheben der Mapping von einer angegebenen Resolver-Abfrageprotokollierungskonfiguration zu einer angegebenen VPC	Write	resolver-query-log-config*		
DisassociateResolverRule	Gewährt die Berechtigung zum Entfernen der Verknüpfung zwischen einer angegebenen Resolver-Regel und einer angegebenen VPC	Write	resolver-rule*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetFirewallConfig	Gewährt die Berechtigung zum Abrufen von Informationen zu einer bestimmten Firewall-Konfig.	Read	firewall-config*		ec2:DescribeVpcs
GetFirewallDomainList	Gewährt die Berechtigung zum Abrufen von Informationen über eine bestimmte Firewall-Domain-Liste	Read	firewall-domain-list*		
GetFirewallRuleGroup	Gewährt die Berechtigung zum Abrufen von Informationen über eine bestimmte Firewall-Regelgruppe.	Read	firewall-rule-group*		
GetFirewallRuleGroupAssociation	Gewährt die Berechtigung zum Abrufen von Informationen über eine Verknüpfung zwischen einer angegebenen Firewall-Regelgruppe und einer VPC	Read	firewall-rule-group-association*		
GetFirewallRuleGroupPolicy	Gewährt die Berechtigung zum Abrufen von Informationen über eine bestimmte Firewall-Regelgruppenrichtlinie, die die Vorgänge und Ressourcen der Firewall-Regelgruppe angibt, die Sie einem anderen AWS-Konto erlauben möchten.	Lesen	firewall-rule-group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetOutpostResolver	Gewährt die Berechtigung zum Abrufen von Informationen über einen bestimmten Route-53-Resolver in Outposts	Lesen	outpost-resolver*		
GetResolverConfig	Gewährt die Berechtigung zum Abrufen des Resolver-Config-Status innerhalb der angegebenen Ressource	Lesen	resolver-config*		ec2:DescribeVpcs
GetResolverDnssecConfig	Gewährt die Berechtigung zum Abrufen des Status der DNSSEC-Validierungsunterstützung für DNS-Abfragen innerhalb der angegebenen Ressource	Read	resolver-dnssec-config*		
GetResolverEndpoint	Gewährt die Berechtigung zum Abrufen von Informationen zu einem bestimmten Resolver-Endpunkt, wie z. B. ob es sich um einen eingehenden oder ausgehenden Resolver-Endpunkt handelt, und der IP-Adressen in Ihrer VPC, an die DNS-Abfragen auf dem Weg in oder aus Ihrer VPC weitergeleitet werden	Read	resolver-endpoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetResolverQueryLogConfig	Gewährt die Berechtigung zum Abrufen von Informationen über eine angegebene Konfiguration der Resolver-Abfrageprotokollierung, z. B. die Anzahl der VPCs, für die die Konfiguration Abfragen protokolliert, und den Speicherort, an den die Protokolle gesendet werden	Read	resolver-query-log-config*		ec2:DescribeVpcs
GetResolverQueryLogConfigAssociation	Gewährt die Berechtigung zum Abrufen von Informationen über eine angegebene Mapping einer Resolver-Abfrageprotokollierungskonfiguration zu einer Amazon VPC. Wenn Sie eine VPC mit einer Abfrageprotokollierungskonfiguration verknüpfen, protokolliert Resolver DNS-Abfragen, die aus dieser VPC stammen	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetResolverQueryLogConfigPolicy	Gewährt die Berechtigung zum Abrufen von Informationen zu einer angegebenen Richtlinie für die Protokollierung von Resolver-Abfragen, die die Vorgänge und Ressourcen angibt, deren Verwendung durch ein anderes AWS-Konto Sie zulassen möchten	Read	resolver-query-log-config*		
GetResolverRule	Gewährt die Berechtigung zum Abrufen von Informationen zu einer bestimmten Resolver-Regel, z. B. den Domain-Namen, für den die Regel DNS-Abfragen weiterleitet, und die IP-Adresse, an die Abfragen weitergeleitet werden	Read	resolver-rule*		
GetResolverRuleAssociation	Gewährt die Berechtigung zum Abrufen von Informationen über eine Verknüpfung zwischen einer angegebenen Resolver-Regel und einer VPC	Read	resolver-rule*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetResolverRulePolicy	Gewährt die Berechtigung zum Abrufen von Informationen über eine Resolver-Regelrichtlinie, die die Auflösungsvorgänge und -ressourcen angibt, die Sie für ein anderes AWS-Konto zulassen möchten	Read	resolver-rule*		
ImportFirewallDomains	Gewährt die Berechtigung zum Hinzufügen, Entfernen oder Ersetzen von Firewall-Domains in einer Firewall-Domain-Liste	Write	firewall-domain-list*		
ListFirewallConfigs	Gewährt die Berechtigung zum Auflisten aller Firewall-Konfigurationen, die das aktuelle AWS-Konto überprüfen kann.	List			ec2:DescribeVpcs
ListFirewallDomainLists	Gewährt die Berechtigung zum Auflisten aller Firewall-Domain-Liste, die das aktuelle AWS-Konto verwenden kann.	List			
ListFirewallDomains	Gewährt die Berechtigung zum Auflisten der gesamten Firewall-Domain unter einer angegebenen Firewall-Domain-Liste	List	firewall-domain-list*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListFirewallRuleGroupAssociations	Gewährt die Berechtigung zum Auflisten von Informationen über Verknüpfungen zwischen Amazon VPCs und der Firewall-Regelgruppe.	List			
ListFirewallRuleGroups	Gewährt die Berechtigung zum Auflisten aller Firewall-Regelgruppen, die das aktuelle AWS-Konto verwenden kann.	List			
ListFirewallRules	Gewährt die Berechtigung zum Auflisten aller Firewall-Regeln unter einer angegebenen Firewall-Regelgruppe.	Auflisten	firewall-rule-group*		
ListOutpostResolvers	Gewährt die Berechtigung zum Auflisten aller Route-53-Resolvers in Outposts, die mit dem aktuellen AWS-Konto erstellt wurden	Auflisten			
ListResolverConfigs	Gewährt die Berechtigung zum Auflisten der Resolver-Config-Status	Auflisten	resolver-config*		ec2:DescribeVpcs
ListResolverDnssecConfigs	Gewährt die Berechtigung zum Auflisten des Status der DNSSEC-Validierungsunterstützung für DNS-Abfragen	Auflisten	resolver-dnssec-config*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListResolverEndpointIpAddresses	Gewährt die Berechtigung zum Auflisten der IP-Adressen, die DNS-Abfragen auf dem Weg zu Ihrem Netzwerk (ausgehend) oder Ihrer VPCs (eingehend) durchlaufen, für einen angegebenen Resolver-Endpunkt	Auflisten	resolver-endpoint*		
ListResolverEndpoints	Gewährt die Berechtigung zum Auflisten aller Resolver-Endpunkte, die mit dem aktuellen AWS-Konto erstellt wurden	List			
ListResolverQueryLogConfigAssociations	Gewährt die Berechtigung, Informationen über Mappings von Amazon VPCs und Konfigurationen für die Abfrageprotokollierung aufzulisten	List			ec2:DescribeVpcs
ListResolverQueryLogConfigs	Gewährt die Berechtigung zum Auflisten von Informationen zu den angegebenen Abfrageprotokollierkonfigurationen, die definieren, wo Resolver DNS-Abfrageprotokolle speichern soll, und zur Angabe der VPCs, für die Sie Abfragen protokollieren möchten	List			ec2:DescribeVpcs

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListResolverRuleAssociations	Gewährt die Berechtigung zum Auflisten der Verknüpfungen, die zwischen Resolver-Regeln und VPCs mit dem aktuellen AWS-Konto erstellt wurden	List			ec2:DescribeVpcs
ListResolverRules	Gewährt die Berechtigung zum Auflisten der Resolver-Regeln, die mit dem aktuellen AWS-Konto erstellt wurden	List			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags, die Sie mit der angegebenen Ressource verknüpft haben	Read	firewall-domain-list		
			firewall-rule-group		
			firewall-rule-group-association		
			outpost-resolver		
			resolver-endpoint		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			resolver-query-log-config		
			resolver-rule		
PutFirewallRuleGroupPolicy	Gewährt die Berechtigung zum Angeben eines AWS-Kontos, für das Sie eine Firewall-Regelgruppe freigeben möchten, der Firewall-Regelgruppe, die Sie freigeben möchten, und der Vorgänge, die das Konto für die Konfiguration ausführen soll	Berechtigungsverwaltung	firewall-rule-group*		
PutResolverQueryLogConfigPolicy	Gewährt die Berechtigung zum Angeben eines AWS-Kontos, für das Sie eine Abfrageprotokollierungskonfiguration freigeben möchten, der Konfiguration der Abfrageprotokollierung, die Sie freigeben möchten, und der Vorgänge, die das Konto für die Konfiguration ausführen soll	Berechtigungsverwaltung	resolver-query-log-config*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutResolverRulePolicy	Gewährt die Berechtigung zur Angabe eines AWS-Kontos, für das Sie Regeln freigeben möchten, der Resolver-Regeln, die Sie freigeben möchten, und der Vorgänge, die das Konto für diese Regeln ausführen soll	Berechtigungsverwaltung	resolver-rule*		
TagResource	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Tags zu einer bestimmten Ressource	Markieren	firewall-config		
			firewall-domain-list		
			firewall-rule-group		
			firewall-rule-group-association		
			outpost-resolver		
			resolver-dnssec-config		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			resolver-endpoint		
			resolver-query-log-config		
			resolver-rule		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen eines oder mehrerer Tags von einer bestimmten Ressource	Markieren	firewall-config		
			firewall-domain-list		
			firewall-rule-group		
			firewall-rule-group-association		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			outpost-resolver		
			resolver-dnssec-config		
			resolver-endpoint		
			resolver-query-log-config		
			resolver-rule		
				aws:TagKeys	
UpdateFirewallConfig	Gewährt die Berechtigung zum Aktualisieren ausgewählter Einstellungen für eine Firewall-Konfiguration.	Write	firewall-config*		ec2:DescribeVpcs
UpdateFirewallDomains	Gewährt die Berechtigung zum Hinzufügen, Entfernen oder Ersetzen von Firewall-Domains in einer Firewall-Domain-Liste	Write	firewall-domain-list*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateFirewallRule	Gewährt die Berechtigung zum Aktualisieren ausgewählter Einstellungen für eine Firewall-Regel in einer Firewall-Regelgruppe.	Write	firewall-domain-list*		
			firewall-rule-group*		
UpdateFirewallRuleGroupAssociation	Gewährt die Berechtigung zum Aktualisieren ausgewählter Einstellungen für eine Firewall-Regelgruppenmapping.	Schreiben	firewall-rule-group-association*		
UpdateOutpostResolver	Gewährt die Berechtigung zum Aktualisieren der Einstellungen für einen bestimmten Route-53-Resolver in Outposts	Schreiben	outpost-resolver*		
UpdateResolverConfig	Gewährt die Berechtigung zum Aktualisieren des Resolver-Config-Status innerhalb der angegebenen Ressource	Schreiben	resolver-config*		ec2:DescribeVpcs
UpdateResolverDnssecConfig	Gewährt die Berechtigung zum Aktualisieren des Status der DNSSEC-Validierungsunterstützung für DNS-Abfragen innerhalb der angegebenen Ressource	Write	resolver-dnssec-config*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateResolverEndpoint	Gewährt die Berechtigung zum Aktualisieren von ausgewählten Einstellungen für einen eingehenden oder ausgehenden Resolver-Endpunkt	Write	resolver-endpoint*		ec2:AssignIpv6Addresses ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:ModifyNetworkInterfaceAttribute ec2:UnassignIpv6Addresses
UpdateResolverRule	Gewährt die Berechtigung zum Aktualisieren der Einstellungen für eine angegebene Resolver-Regel	Write	resolver-rule*		

Von Amazon Route 53 Resolver definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
resolver-dnssec-config	`arn:${Partition}:route53resolver:${Region}:${Account}:resolver-dnssec-config/${ResourceId}`	aws:ResourceTag/${TagKey}
resolver-query-log-config	`arn:${Partition}:route53resolver:${Region}:${Account}:resolver-query-log-config/${ResourceId}`	aws:ResourceTag/${TagKey}
resolver-rule	`arn:${Partition}:route53resolver:${Region}:${Account}:resolver-rule/${ResourceId}`	aws:ResourceTag/${TagKey}
resolver-endpoint	`arn:${Partition}:route53resolver:${Region}:${Account}:resolver-endpoint/${ResourceId}`	aws:ResourceTag/${TagKey}
firewall-rule-group	`arn:${Partition}:route53resolver:${Region}:${Account}:firewall-rule-group/${ResourceId}`	aws:ResourceTag/${TagKey}
firewall-rule-group-association	`arn:${Partition}:route53resolver:${Region}:${Account}:firewall-rule-group-association/${ResourceId}`	aws:ResourceTag/${TagKey}
firewall-domain-list	`arn:${Partition}:route53resolver:${Region}:${Account}:firewall-domain-list/${ResourceId}`	aws:ResourceTag/${TagKey}
firewall-config	`arn:${Partition}:route53resolver:${Region}:${Account}:firewall-config/${ResourceId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
resolver-config	`arn:${Partition}:route53resolver:${Region}:${Account}:resolver-config/${ResourceId}`	
outpost-resolver	`arn:${Partition}:route53resolver:${Region}:${Account}:outpost-resolver/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Route 53 Resolver

Amazon Route 53 Resolver definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüsselwertpaaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon S3

Amazon S3 (Servicepräfix: `s3`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon S3 definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWSzu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AbortMultipartUpload	Gewährt die Berechtigung zum Abbrechen eines mehrteiligen Uploads	Write	object*		
				s3:DataAccessPointArn s3:AccessGrantsInstanceArn s3:DataAccessPointAccount	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
AssociateAccessGrantsIdentityCenter	Gewährt die Berechtigung zum Zuordnen von Access Grants Identity Center	Write	accessgrantsinstance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
BypassGovernanceRetention	Gewährt die Berechtigung zum Umgehen von Objektaufbewahrungseinstellungen im Governance-Modus	Permissions management	object*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:RequestObjectTag/<key> s3:RequestObjectTagKeys s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:TlsVersion s3:x-amz-acl s3:x-amz-content-sha256 s3:x-amz-copy-source s3:x-amz-grant-full-control s3:x-amz-grant-read s3:x-amz-grant-read-acp s3:x-amz-	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				grant-write s3:x-amz-grant-write-acp s3:x-amz-metadata-directive s3:x-amz-server-side-encryption s3:x-amz-server-side-encryption-aws-kms-key-id s3:x-amz-server-side-	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				encryption-customer-algorithm s3:x-amz-storage-class s3:x-amz-website-redirect-location s3:object-lock-mode s3:object-lock-retain-until-date s3:object-lock-remaining-retention-days	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:object-lock-legal-hold	
CreateAccessGrant	Gewährt die Berechtigung zum Erstellen von Access Grant	Schreiben	accessgrantslocation*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAccessGrantsInstance	Gewährt die Berechtigung zum Erstellen einer Access Grant-Instance	Schreiben	accessgrantsinstance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAccessGrantsLocation	Gewährt die Berechtigung zum Erstellen eines Access Grants-Speicherorts	Schreiben	accessgrantsinstance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAccessPoint	Gewährt die Berechtigung zum Erstellen eines neuen Zugangspunkts	Write	accesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:locationconstraint s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-acl	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:x-amz-content-sha256	
CreateAccessPointForObjectLambda	Gewährt die Berechtigung zum Erstellen eines Objekt-Lambda-fähigen Zugriffspunkts	Write	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateBucket	Gewährt die Berechtigung zum Erstellen eines neuen Buckets.	Write	bucket*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:locationconstraint s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-acl s3:x-amz-content-sha256 s3:x-amz-grant-full-control	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:x-amz-grant-read s3:x-amz-grant-read-acp s3:x-amz-grant-write s3:x-amz-grant-write-acp s3:x-amz-object-ownership	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateJob	Erteilt die Berechtigung zum Erstellen einer neuen Aufgabe in Amazon S3 Batch Operations	Schreiben		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:RequestJobPriority s3:RequestJobOperation aws:TagKeys	iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey}	
CreateMultiRegionAccessPoint	Gewährt die Berechtigung zum Erstellen eines neuen Multi-Region-Zugangspunkts	Schreiben	multiregionaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateStorageLensGroup	Gewährt die Berechtigung zum Erstellen einer Amazon-S3-Storage-Lens-Gruppe	Schreiben		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessGrant	Gewährt die Berechtigung zum Löschen eines Access Grants	Schreiben	accessgrant*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
DeleteAccessGrantsInstance	Gewährt die Berechtigung zum Löschen einer Access Grant-Instance	Schreiben	accessgrantsinstance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
DeleteAccessGrantsInstanceResourcePolicy	Gewährt die Berechtigung zum Lesen einer Access Grants Instance-Ressourcenrichtlinie	Schreiben	accessgrantsinstance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
DeleteAccessGrantsLocation	Gewährt die Berechtigung zum Löschen eines Access Grant-Speicherorts	Schreiben	accessgrantslocation*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
DeleteAccessPoint	Gewährt die Berechtigung zum Löschen des im URI benannten Zugriffspunkts	Write	accesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointArn s3:DataAccessPointAccount s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteAccessPointForObjectLambda	Gewährt die Berechtigung zum Löschen des im URI benannten Objekt-Lambda-fähigen Zugriffspunkts	Write	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointArn s3:DataAccessPointAccount s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteAccessPointPolicy	Gewährt die Berechtigung zum Löschen der Richtlinie auf einem angegebenen Zugriffspunkt	Permissions management	accesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointArn s3:DataAccessPointAccount s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteAccessPointPolicyForObjectLambda	Gewährt die Berechtigung zum Löschen der Richtlinie auf einem angegebenen Objekt-Lambda-fähigen Zugriffspunkt	Permissions management	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointArn s3:DataAccessPointAccount s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteBucket	Gewährt die Berechtigung zum Löschen des im URI benannten Buckets	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteBucketPolicy	Gewährt die Berechtigung zum Löschen der Richtlinie für einen angegebenen Bucket	Permissions management	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
DeleteBucketWebsite	Gewährt die Berechtigung zum Entfernen der Websitekonfiguration für einen Bucket	Write	bucket*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteJobTagging	Erteilt die Berechtigung zum Entfernen von Markierungen aus einer vorhandenen Aufgabe in Amazon S3 Batch Operations	Markieren	job*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:ExistingJobPriority s3:ExistingJobOperation	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteMultiRegionAccessPoint	Gewährt die Berechtigung zum Löschen des im URI benannten Multi-Region-Zugriffspunkts	Schreiben	multiregionaccesspoint*		
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteObject	Gewährt die Berechtigung zum Entfernen der Null-Version eines Objekts und zum Einfügen einer Löschmarkierung, die zur aktuellen Version des Objekts wird.	Write	object*		
				s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteObjectTagging	Gewährt die Berechtigung zum Verwenden der Tagging-Unterquelle, um den gesamten Tag-Satz aus dem angegebenen Objekt zu entfernen.	Markieren	object*		
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:x-amz-content-sha256	
DeleteObjectVersion	Gewährt die Berechtigung zum Entfernen einer bestimmten Version eines Objekts	Write	object*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:x-amz-content-sha256	
DeleteObjectVersionTagging	Erteilt die Berechtigung zum Entfernen des gesamten Tag-Satzes für eine bestimmte Version des Objekts	Markieren	object*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:x-amz-content-sha256	
DeleteStorageLensConfiguration	Erteilt die Berechtigung zum Löschen einer bestehenden Amazon-S3-Storage-Lens-Konfiguration	Write	storagelensconfiguration*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteStorageLensConfigurationTagging	Erteilt die Berechtigung zum Entfernen von Markierungen aus einer vorhandenen Amazon-S3-Storage-Lens-Konfiguration	Tagging	storagelensconfiguration*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
DeleteStorageLensGroup	Gewährt die Berechtigung zum Löschen einer bestehenden S3-Storage-Lens-Gruppe	Schreiben	storagelensgroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeJob	Gewährt die Berechtigung zum Abrufen der Konfigurationsparameter und des Status für eine Batch-Operationsaufgabe	Lesen	job*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
DescribeMultiRegionAccessPointOperation	Gewährt die Berechtigung zum Abrufen der Konfigurationen für einen Zugriffspunkt mit mehreren Regionen	Lesen	multiregionaccesspointrequestarn*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
DissociateAccessGrantsIdentityCenter	Gewährt die Berechtigung zum Trennen von Access Grants Identity Center	Schreiben	accessgrantsinstance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAccelerateConfiguration	Gewährt die Berechtigung zum Verwenden der Accelerate-Unterressource, um den „Transfer Acceleration“-Status eines Buckets – „Enabled“ oder „Suspended“ – zurückzugeben.	Lesen	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetAccessGrant	Gewährt die Berechtigung zum Lesen von Access Grant	Lesen	accessgrant*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
GetAccessGrantsInstance	Gewährt die Berechtigung zum Lesen der Access Grants-Instance	Lesen	accessgrantsinstance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
GetAccessGrantsInstanceForPrefix	Gewährt die Berechtigung zum Lesen der Access Grants-Instance anhand des Präfixes	Lesen	accessgrantsinstance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
GetAccessGrantsInstanceResourcePolicy	Gewährt die Berechtigung zum Lesen einer Access Grants Instance-Ressourcenrichtlinie	Lesen	accessgrantsinstance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
GetAccessGrantsLocation	Gewährt die Berechtigung zum Lesen des Access Grants-Speicherorts	Lesen	accessgrantslocation*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAccessPoint	Gewährt die Berechtigung zum Zurückgeben von Konfigurationsinformationen zum angegebenen Zugriffspunkt	Read		s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAccessPointConfigurationForObjectLambda	Gewährt die Berechtigung zum Abrufen der Konfiguration des Objekt-Lambda-fähigen Zugriffspunkts	Read	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointArn s3:DataAccessPointAccount s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAccessPointForObjectLambda	Gewährt die Berechtigung zum Erstellen eines Objekt-Lambda-fähigen Zugriffspunkts	Read	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAccessPointPolicy	Gewährt die Berechtigung zum Zurückgeben der Zugriffspunktrichtlinie, die dem angegebenen Zugriffspunkt zugeordnet ist	Read	accesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAccessPointPolicyForObjectLambda	Gewährt die Berechtigung zum Zurückgeben der Zugriffspunktrichtlinie, die dem angegebenen Objekt-Lambda-fähigen Zugriffspunkt zugeordnet ist	Read	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAccessPointPolicyStatus	Gewährt die Berechtigung zum Zurückgeben des Richtlinienstatus für eine bestimmte Zugriffspunktrichtlinie	Read	accesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAccessPointPolicyStatusForObjectLambda	Gewährt die Berechtigung zum Zurückgeben des Richtlinienstatus für eine bestimmte Objekt-Lambda-Zugriffspunktrichtlinie	Lesen	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAccountPublicAccessBlock	Gewährt die Berechtigung zum Abrufen der PublicAccessBlock Konfiguration für ein AWS-Konto	Lesen		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAnalyticsConfiguration	Erteilt die Berechtigung zum Abrufen einer Analytics-Konfiguration aus einem Amazon-S3-Bucket, identifiziert durch die Analytics-Konfigurations-ID	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBucketAcl	Erteilt die Berechtigung zum Verwenden der ACL-Unterquelle zum Zurückgeben der Zugriffskontrollliste (Access Control List, ACL) eines Amazon-S3-Buckets	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBucketCORS	Erteilt die Berechtigung zum Zurückgeben der CORS-Konfigurationsinformationen für einen Amazon-S3-Bucket	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBucketLocation	Erteilt die Berechtigung zum Zurückgeben der Region, in der sich ein Amazon-S3-Bucket befindet.	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBucketLogging	Erteilt die Berechtigung zum Zurückgeben des Protokollierungsstatus eines Amazon-S3-Buckets und der Berechtigungen, die Benutzer zum Anzeigen oder Ändern dieses Status haben	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBucketNotification	Erteilt die Berechtigung zum Abrufen der Benachrichtigungskonfiguration eines Amazon-S3-Buckets	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBucketObjectLockConfiguration	Erteilt die Berechtigung zum Abrufen der Object Lock-Konfiguration eines Amazon-S3-Buckets	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:signatureversion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBucketOwnershipControls	Gewährt die Berechtigung zum Abrufen von Kontrollen zur Eigentümerschaft in einem Bucket	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetBucketPolicy	Gewährt die Berechtigung zum Zurückgeben der Richtlinie des angegebenen Buckets	Read	bucket*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBucketPolicyStatus	Erteilt die Berechtigung zum Abrufen des Richtlinienstatus für einen bestimmten Amazon-S3-Bucket, der angibt, ob der Bucket öffentlich ist	Lesen	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBucketPublicAccessBlock	Gewährt die Berechtigung zum Abrufen der PublicAccessBlock Konfiguration für einen Amazon S3-Bucket	Lesen	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBucketRequestPayment	Erteilt die Berechtigung zum Zurückgeben der Anforderungszahlungskonfiguration für einen Amazon-S3-Bucket	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBucketTagging	Erteilt die Berechtigung zum Zurückgeben des Tag-Satzes, der einem Amazon-S3-Bucket zugeordnet ist	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBucketVersioning	Erteilt die Berechtigung zum Zurückgeben des Versionssteuerungsstatus eines Amazon-S3-Buckets	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBucketWebsite	Erteilt die Berechtigung zum Zurückgeben der Website-Konfiguration für einen Amazon-S3-Bucket	Lesen	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetDataAccess	Gewährt die Berechtigung zum Zugriff	Lesen	accessgrantsinstance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetEncryptionConfiguration	Erteilt die Berechtigung zum Zurückgeben der Standard-Verschlüsselungskonfiguration eines Amazon-S3-Buckets	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetIntelligentTieringConfiguration	Gewährt die Berechtigung zum Abrufen oder Auflisten aller Amazon S3 Intelligent Tiering-Konfigurationen in einem S3-Bucket	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetInventoryConfiguration	Erteilt die Berechtigung zum Zurückgeben einer Inventarkonfiguration aus einem Amazon-S3-Bucket, die durch die Inventarkonfigurations-ID gekennzeichnet ist.	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetJobTagging	Erteilt die Berechtigung zum Zurückgeben des Tag-Satzes eines vorhandenen Auftrags in Amazon S3 Batch Operations	Read	job*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetLifecycleConfiguration	Erteilt die Berechtigung zum Zurückgeben der Lebenszyklus-Konfigurationsinformationen, die in einem Amazon-S3-Bucket festgelegt sind.	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetMetricsConfiguration	Erteilt die Berechtigung zum Abrufen einer Metrik-Konfiguration aus einem Amazon-S3-Bucket	Lesen	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetMultiRegionAccessPoint	Gewährt die Berechtigung zum Zurückgeben von Konfigurationsinformationen zum angegebenen Multi-Region-Zugriffspunkt	Lesen	multiregionaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
GetMultiRegionAccessPointPolicy	Gewährt die Berechtigung zum Zurückgeben der Zugriffspunktrichtlinie, die dem angegebenen Multi-Region-Zugriffspunkt zugeordnet ist	Lesen	multiregionaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
GetMultiRegionAccessPointPolicyStatus	Gewährt die Berechtigung zum Zurückgeben des Richtlinienstatus für eine bestimmte Multi-Region-Zugriffspunktrichtlinie	Lesen	multiregionaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
GetMultiRegionAccessPointRoutes	Gewährt die Berechtigung zum Abrufen der Routenkonfigurationen für einen Zugriffspunkt mit mehreren Regionen	Lesen	multiregionaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
GetObject	Gewährt die Berechtigung zum Abrufen von Objekten aus Amazon S3	Read	object*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetObjectAcl	Gewährt die Berechtigung zum Zurückgeben der Zugriffskontrollliste (Access Control List, ACL) eines Objekts	Lesen	object*		
				s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:TlsVersion s3:x-amz-content-sha256	
GetObjectAttributes	Gewährt die Berechtigung zum Abrufen von Attributen, die sich auf ein bestimmtes Objekt beziehen	Lesen	object*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				content-sha256	
GetObjectLegalHold	Gewährt die Berechtigung zum Abrufen des aktuellen „Legal Hold“-Status eines Objekts	Read	object*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetObjectRetention	Gewährt die Berechtigung zum Abrufen der Aufbewahrungseinstellungen für ein Objekt	Read	object*		
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetObjectTagging	Erteilt die Berechtigung zum Zurückgeben des Tag-Satzes eines Objekts	Read	object*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				content-sha256	
GetObjectTorrent	Gewährt die Berechtigung zum Zurückgeben von Torrent-Dateien aus einem Amazon-S3-Bucket	Read	object*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetObjectVersion	Gewährt die Berechtigung zum Abrufen einer bestimmten Version eines Objekts	Read	object*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:TlsVersion s3:versionid s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetObjectVersionAcl	Gewährt die Berechtigung zum Zurückgeben der Zugriffskontrollliste (Access Control List, ACL) einer bestimmten Objektversion	Lesen	object*		
				s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:TlsVersion s3:versionid s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetObjectVersionAttributes	Gewährt die Berechtigung zum Abrufen von Attributen, die sich auf eine bestimmte Version eines Objekts beziehen	Lesen	object*	s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:versionid s3:x-amz-content-sha256	
GetObjectVersionForReplication	Gewährt die Berechtigung zum Replizieren sowohl unverschlüsselter Objekte als auch von Objekten, die mit SSE-S3 oder SSE-KMS verschlüsselt sind.	Read	object*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetObjectVersionTagging	Erteilt die Berechtigung zum Zurückgeben des Tag-Satzes für eine bestimmte Version des Objekts	Read	object*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:x-amz-content-sha256	
GetObjectVersionTorrent	Gewährt die Berechtigung zum Abrufen von Torrent-Dateien zu einer anderen Version mithilfe der VersionID-Unterquelle	Read	object*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetReplicationConfiguration	Erteilt die Berechtigung zum Abrufen der in einem Amazon-S3-Bucket festgelegten Replikations-Konfigurationsinformationen	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetStorageLensConfiguration	Erteilt die Berechtigung zum Abrufen einer Amazon-S3-Storage-Lens-Konfiguration	Read	storagelensconfiguration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetStorageLensConfigurationTagging	Erteilt die Berechtigung zum Abrufen des Tag-Satzes einer bestehenden Amazon-S3-Storage-Lens-Konfiguration	Read	storagelensconfiguration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetStorageLensDashboard	Erteilt die Berechtigung zum Abrufen eines Amazon-S3-Storage-Lens-Dashboards	Lesen	storagelensconfiguration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetStorageLensGroup	Gewährt die Berechtigung zum Abrufen einer Amazon-S3-Storage-Lens-Gruppe	Lesen	storagelensgroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
InitiateReplication [nur Berechtigung]	Erteilt die Berechtigung, den Replikationsprozess zu initiieren, indem der Replikationsstatus eines Objekts als „Ausstehend“ festgelegt wird	Schreiben	object*		
				s3:ResourceAccount	
ListAccessGrants	Gewährt die Berechtigung zum Auflisten von Access Grant	Auflisten	accessgrantsinstance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAccessGrantsInstances	Gewährt die Berechtigung zum Auflisten von Access Grants-Instances	Auflisten		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
ListAccessGrantsLocations	Gewährt die Berechtigung zum Auflisten von Access Grants-Speicherorten	Auflisten	accessgrantsinstance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAccessPoints	Gewährt die Berechtigung zum Auflisten von Zugriffspunkten	Auflisten		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAccessPointsForObjectLambda	Gewährt die Berechtigung zum Auflisten von Objekt-Lambda-fähigen Zugriffspunkten	Auflisten		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAllMyBuckets	Gewährt die Berechtigung zum Auflisten aller Buckets, die dem authentifizierten Sender der Anforderung gehören.	List		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
ListBucket	Erteilt die Berechtigung zum Auflisten einiger oder aller Objekte in einem Amazon-S3-Bucket (bis zu 1000)	List	bucket*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:delimiter s3:max-keys s3:prefix s3:ResourceAccount s3:signatureAge	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
ListBucketMultipartUploads	Gewährt die Berechtigung zum Auflisten in Bearbeitung befindlicher mehrteilige Uploads	List	bucket*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				content-sha256	
ListBucketVersions	Erteilt die Berechtigung zum Auflisten von Metadaten zu allen Versionen von Objekten in einem Amazon-S3-Bucket	List	bucket*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:delimiter s3:max-keys s3:prefix s3:ResourceAccount s3:signatureAge	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
ListJobs	Gewährt die Berechtigung zum Auflisten aktueller und kürzlich beendeter Aufgaben	Auflisten		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListMultiRegionAccessPoints	Gewährt die Berechtigung zum Auflisten von Multi-Region-Zugriffspunkten	Auflisten		s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
ListMultipartUploadParts	Gewährt die Berechtigung zum Auflisten der Teile, die für einen bestimmten mehrteiligen Upload hochgeladen wurden	List	object*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				content-sha256	
ListStorageLensConfigurations	Erteilt die Berechtigung zum Auflisten von Amazon-S3-Storage-Lens-Konfigurationen	Auflisten		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListStorageLensGroups	Gewährt die Berechtigung zum Auflisten von S3-Storage-Lens-Gruppen	Auflisten		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags, die einer bestimmten Ressource angefügt sind	Auflisten	accessgrant		
			accessgrantsinstance		
			accessgrantslocation		
			storagelensgroup		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ObjectOwnerOverrideToBucketOwner	Gewährt die Berechtigung zum Ändern der Replikat-Eigentümerschaft	Permissions management	object*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutAccelerateConfiguration	Gewährt die Berechtigung zum Verwenden der Accelerate-Unterquelle zum Festlegen des Transfer Acceleration-Status eines vorhandenen S3-Buckets	Schreiben	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
PutAccessGrantsInstanceResourcePolicy	Gewährt die Berechtigung zum Setzen einer Access Grants-Instance Ressourcenrichtlinie	Schreiben	accessgrantsinstance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
PutAccessPointConfigurationForObjectLambda	Gewährt die Berechtigung zum Festlegen der Konfiguration des Objekt-Lambda-fähigen Zugriffspunkts	Write	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointArn s3:DataAccessPointAccount s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutAccessPointPolicy	Gewährt die Berechtigung zum Zuordnen einer Zugriffsrichtlinie zu einem angegebenen Zugriffspunkt	Permissions management	accesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutAccessPointPolicyForObjectLambda	Gewährt die Berechtigung zum Zuordnen einer Zugriffsrichtlinie zu einem angegebenen Objekt-Lambda-fähigen Zugriffspunkt	Berechtigungsverwaltung	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutAccessPointPublicAccessBlock	Gewährt die Berechtigung zum Zuordnen von Blockkonfigurationen für den öffentlichen Zugriff zu einem angegebenen Zugriffspunkt, während ein Zugriffspunkt erstellt wird	Berechtigungsverwaltung			
PutAccountPublicAccessBlock	Gewährt die Berechtigung zum Erstellen oder Ändern der PublicAccessBlock Konfiguration für ein AWS-Konto	Berechtigungsverwaltung		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutAnalyticsConfiguration	Gewährt die Berechtigung zum Festlegen einer Analytics-Konfiguration für den Bucket, angegeben durch die Analytics-Konfigurations-ID	Write	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutBucketAcl	Gewährt die Berechtigung zum Einrichten von Berechtigungen auf einem bestehenden Bucket mithilfe von Zugriffskontrolllisten (ACLs)	Permissions management	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-acl s3:x-amz-content-sha256 s3:x-amz-grant-full-control s3:x-amz-	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				grant-read s3:x-amz-grant-read-acp s3:x-amz-grant-write s3:x-amz-grant-write-acp	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutBucketCORS	Erteilt die Berechtigung zum Festlegen der CORS-Konfiguration für einen Amazon-S3-Bucket	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutBucketLogging	Erteilt die Berechtigung zum Festlegen der Protokollierungsparameter für einen Amazon-S3-Bucket	Write	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutBucketNotification	Erteilt die Berechtigung zum Erhalt von Benachrichtigungen, wenn bestimmte Ereignisse in einem Amazon-S3-Bucket eintreten	Write	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutBucketObjectLockConfiguration	Gewährt die Berechtigung zum Setzen der Object Lock-Konfiguration auf einem bestimmten Bucket	Schreiben	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:TlsVersion s3:signatureversion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutBucketOwnershipControls	Gewährt die Berechtigung zum Hinzufügen, Ersetzen oder Löschen von Kontrollen zur Eigentümerschaft in einem Bucket	Schreiben	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutBucketPolicy	Gewährt die Berechtigung zum Hinzufügen oder Ersetzen einer Bucket-Richtlinie für einen Bucket	Berechtigungsverwaltung	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutBucketPublicAccessBlock	Gewährt die Berechtigung zum Erstellen oder Ändern der PublicAccessBlock Konfiguration für einen bestimmten Amazon S3-Bucket	Berechtigungsverwaltung	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutBucketRequestPayment	Gewährt die Berechtigung zum Festlegen der Anforderungszahlungskonfiguration eines Buckets	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutBucketTagging	Erteilt die Berechtigung zum Hinzufügen eines Satzes von Markierungen zu einem vorhandenen Amazon-S3-Bucket	Markieren	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutBucketVersioning	Erteilt die Berechtigung zum Festlegen des Versionssteuerungsstatus eines vorhandenen Amazon-S3-Buckets	Write	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutBucketWebsite	Gewährt die Berechtigung zum Festlegen der Konfiguration der Website, die in der Website-Unterressource angegeben ist	Write	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutEncryptionConfiguration	Erteilt die Berechtigung zum Festlegen der Verschlüsselungskonfiguration für einen Amazon-S3-Bucket	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutIntelligentTieringConfiguration	Gewährt die Berechtigung, eine Amazon S3 Intelligent Tiering-Konfiguration zu erstellen, zu aktualisieren oder zu löschen	Write	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutInventoryConfiguration	Gewährt die Berechtigung zum Hinzufügen einer Inventarkonfiguration zu dem Bucket, identifiziert durch die Inventar-ID	Write	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:InventoryAccessibleOptionalFields	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutJobTagging	Erteilt die Berechtigung zum Ersetzen von Markierungen für eine vorhandene Aufgabe in Amazon S3 Batch Operations	Markieren	job*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:ExistingJobPriority s3:ExistingJobOperation aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey}	
PutLifecycleConfiguration	Gewährt die Berechtigung zum Erstellen einer neuen Lebenszyklus-Konfiguration für den Bucket oder zum Ersetzen einer vorhandenen Lebenszyklus-Konfiguration	Schreiben	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutMetricsConfiguration	Gewährt die Berechtigung zum Festlegen oder Aktualisieren einer Metrikkonfiguration für die CloudWatch Anforderungsmetriken aus einem Amazon S3-Bucket	Schreiben	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
PutMultiRegionAccessPointPolicy	Gewährt die Berechtigung zum Zuordnen einer Zugriffsrichtlinie zu einem angegebenen Multi-Region-Zugriffspunkt	Berechtigungsverwaltung	multiregionaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
PutObject	Gewährt die Berechtigung zum Hinzufügen eines Objekts zu einem Bucket	Schreiben	object*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:RequestObjectTag/<key> s3:RequestObjectTagKeys s3:authType s3:ResourceAccount s3:signatureAge	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:signatureversion s3:TlsVersion s3:x-amz-acl s3:x-amz-content-sha256 s3:x-amz-copy-source s3:x-amz-grant-full-control s3:x-amz-grant-read s3:x-amz-grant-read-acp	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:x-amz-grant-write s3:x-amz-grant-write-acp s3:x-amz-metadata-directive s3:x-amz-server-side-encryption s3:x-amz-server-side-encryption-aws-kms-key-id s3:x-amz-	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				server-side-encryption-customer-algorithm s3:x-amz-storage-class s3:x-amz-website-redirect-location s3:object-lock-mode s3:object-lock-retain-until-date s3:object-lock-remaining-retention-days	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:object-lock-legal-hold	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutObjectAcl	Gewährt die Berechtigung zum Festlegen der Berechtigungen für Zugriffskontrolllisten (Access Control Lists, ACL) für neue oder vorhandene Objekte in einem S3 Bucket	Berechtigungsverwaltung	object*	s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:TlsVersion s3:x-amz-acl s3:x-amz-content-sha256 s3:x-amz-grant-full-control s3:x-amz-grant-read s3:x-amz-grant-read-acp s3:x-amz-grant-write s3:x-amz-	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				grant-write-acp s3:x-amz-storage-class	
PutObjectLegalHold	Gewährt die Berechtigung zum Anwenden einer Legal Hold Konfiguration auf das angegebene Objekt	Write	object*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:object-lock-legal-hold	
PutObjectRetention	Gewährt die Berechtigung zum Platzieren einer Objektaufbewahrungskonfiguration auf einem Objekt	Write	object*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:object-lock-mode s3:object-lock-retain-until-date s3:object-lock-remaining-retention-days	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutObjectTagging	Erteilt die Berechtigung zum Festlegen des bereitgestellten Tag-Satzes für ein Objekt, das bereits in einem Bucket vorhanden ist	Markieren	object*	s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:RequestObjectTag/<key> s3:RequestObjectTagKeys s3:authType s3:ResourceAccount s3:signatureAge	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutObjectVersionAcl	Erteilt die Berechtigung zum Verwenden der ACL (Access Control List)-Unterquelle zum Festlegen der Access-Control-List-Berechtigungen für ein Objekt, das bereits in einem Bucket vorhanden ist	Permissions management	object*	s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:TlsVersion s3:versionid s3:x-amz-acl s3:x-amz-content-sha256 s3:x-amz-grant-full-control s3:x-amz-grant-read s3:x-amz-grant-read-acp s3:x-amz-grant-write	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:x-amz-grant-write-acp s3:x-amz-storage-class	
PutObjectVersionTagging	Erteilt die Berechtigung zum Festlegen des bereitgestellten Tag-Satzes für eine bestimmte Version eines Objekts	Markieren	object*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:RequestObjectTag/<key> s3:RequestObjectTagKeys s3:authType s3:ResourceAccount s3:signatureAge	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:signatureversion s3:TlsVersion s3:versionid s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutReplicationConfiguration	Gewährt die Berechtigung zum Erstellen einer neuen Replikations-Konfiguration oder zum Ersetzen einer vorhandenen Replikations-Konfiguration	Write	bucket*		iam:PassRole
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutStorageLensConfiguration	Erteilt die Berechtigung zum Erstellen oder Aktualisieren einer Amazon-S3-Storage-Lens-Konfiguration	Write		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:TagKeys aws:RequestTag/${TagKey}	
PutStorageLensConfigurationTagging	Erteilt die Berechtigung zum Setzen oder Ersetzen von Markierungen auf eine vorhandene Amazon-S3-Storage-Lens-Konfiguration	Markieren	storagelensconfiguration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Replicate Delete	Gewährt die Berechtigung zum Replizieren von Löschmarkierungen auf den Ziel-Bucket	Write	object*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Replicate Object	Gewährt die Berechtigung zum Replizieren von Objekten und Objekt-Markierungen auf den Ziel-Bucket	Write	object*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:x-amz-server-side-encryption s3:x-amz-server-side-	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				encryption-aws-kms-key-id s3:x-amz-server-side-encryption-customer-algorithm	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ReplicateTags	Gewährt die Berechtigung zum Replizieren von Objekt-Markierungen auf den Ziel-Bucket	Markieren	object*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
RestoreObject	Gewährt die Berechtigung zum Wiederherstellen einer archivierten Kopie eines Objekts in Amazon S3	Schreiben	object*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SubmitMultiRegionAccessPointRoutes	Gewährt die Berechtigung zum Einreichen eines Multi-Regions-Zugriffspunkts auf einen Multi-Regions-Zugriffspunkt	Schreiben	multiregionaccesspoint*		
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zur angegebenen Ressource	Tagging	accessgrant		
			accessgrantsinstance		
			accessgrantslocation		
			storagelensgroup		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus der angegebenen Ressource	Tagging	accessgrant accessgrantsinstance		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			accessgrantslocation		
			storagelensgroup		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:TagKeys	
UpdateAccessGrantsLocation	Gewährt die Berechtigung zum Aktualisieren eines Access Grants-Speicherorts	Schreiben	accessgrantslocation*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
UpdateJobPriority	Gewährt die Berechtigung zum Aktualisieren der Priorität einer vorhandenen Aufgabe	Schreiben	job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:RequestJobPriority s3:ExistingJobPriority s3:ExistingJobOperation	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateJobStatus	Gewährt die Berechtigung zum Aktualisieren des Status der angegebenen Aufgabe	Schreiben	job*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:ExistingJobPriority s3:ExistingJobOperation s3:JobSuspendedCause	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateStorageLensGroup	Gewährt die Berechtigung zum Aktualisieren einer vorhandenen S3-Storage-Lens-Gruppe	Schreiben	storagelensgroup*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Von Amazon S3 definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
accesspoint	arn:${Partition}:s3:${Region}:${Account}:accesspoint/${AccessPointName}	
bucket	arn:${Partition}:s3:::${BucketName}	
object	arn:${Partition}:s3:::${BucketName}/${ObjectName}	
job	arn:${Partition}:s3:${Region}:${Account}:job/${JobId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
storagelensconfiguration	arn:${Partition}:s3:${Region}:${Account}:storage-lens/${ConfigId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
storagelensgroup	arn:${Partition}:s3:${Region}:${Account}:storage-lens-group/${Name}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
objectlambdaaccesspoint	arn:${Partition}:s3-object-lambda:${Region}:${Account}:accesspoint/${AccessPointName}	

Ressourcentypen	ARN	Bedingungsschlüssel
multiregionalaccesspoint	arn:${Partition}:s3::${Account}:accesspoint/${AccessPointAlias}	
multiregionalaccesspointrequestarn	arn:${Partition}:s3:us-west-2:${Account}:async-request/mrap/${Operation}/${Token}	
accessgrantsinstance	arn:${Partition}:s3:${Region}:${Account}:access-grants/default	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
accessgrantslocation	arn:${Partition}:s3:${Region}:${Account}:access-grants/default/location/${Token}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
accessgrant	arn:${Partition}:s3:${Region}:${Account}:access-grants/default/grant/${Token}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Bedingungsschlüssel für Amazon S3

Amazon S3 definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString
s3:AccessGrantsInstanceArn	Filtert den Zugriff nach dem ARN der Zugriffsgewährungs-Instance	ARN
s3:AccessPointNetworkOrigin	Filtert den Zugriff nach Netzwerkursprung (Internet oder VPC)	String
s3:DataAccessPointAccount	Filtert den Zugriff nach der AWS Konto-ID, die Eigentümer des Zugriffspunkts ist	String
s3:DataAccessPointArn	Filtert den Zugriff nach Amazon-Ressourcenname (ARN) des Zugriffspunkts	ARN

Bedingungsschlüssel	Beschreibung	Typ
s3:ExistingJobOperation	Filtert den Zugriff auf die Aktualisierung der Aufgabenpriorität nach Operation.	String
s3:ExistingJobPriority	Filtert den Zugriff auf das Abbrechen vorhandener Aufgaben nach Prioritätsbereich	Numerischer Wert
s3:ExistingObjectTag/<key>	Filtert den Zugriff nach vorhandenem Objekt-Tag-Schlüssel und -Wert	String
s3:InventoryAccessibleOptionalFields	Filtert den Zugriff, indem beschränkt wird, welche optionalen Metadatenfelder ein Benutzer bei der Konfiguration von S3-Inventory-Berichten hinzufügen kann	ArrayOfString
s3:JobSuspendedCause	Filtert den Zugriff der durch einen bestimmten Abbruchsgrund angehaltenen Aufträge (z. B. AWAITING_CONFIRMATION) zum abbrechen angehaltener Aufträgel	String
s3:RequestJobOperation	Filtert den Zugriff auf das Erstellen von Aufträge nach Operation	String
s3:RequestJobPriority	Filtert den Zugriff auf das Erstellen neuer Aufträge nach Prioritätsbereich	Numerischer Wert
s3:RequestObjectTag/<key>	Filtert den Zugriff nach den Tag-Schlüsseln und -Werten, die Objekten hinzugefügt werden sollen	Zeichenfolge
s3:RequestObjectTagKeys	Filtert den Zugriff nach den Tag-Schlüsseln, die zu Objekten hinzugefügt werden sollen	ArrayOfString
s3:ResourceAccount	Filtert den Zugriff nach der Ressourcenbesitzer AWS-Konto -ID	String

Bedingungsschlüssel	Beschreibung	Typ
s3:TlsVersion	Filtert den Zugriff nach der TLS-Version, die vom Client verwendet wird	Numerischer Wert
s3:authType	Filtert den Zugriff nach Authentifizierungsmethode	Zeichenfolge
s3:delimiter	Filtert den Zugriff nach Trennzeichen-Parameter	Zeichenfolge
s3:locationconstraint	Filtert den Zugriff nach einer bestimmten Region	String
s3:max-keys	Filtert den Zugriff nach der maximalen Anzahl von Schlüsseln, die in einer ListBucket Anforderung zurückgegeben werden	Numerischer Wert
s3:object-lock-legal-hold	Filtert den Zugriff nach dem rechtlichen Haltestatus des Objekts	Zeichenfolge
s3:object-lock-mode	Filtert den Zugriff nach dem Aufbewahrungsmodus des Objekts (Compliance oder Governance)	Zeichenfolge
s3:object-lock-remaining-retention-days	Filtert den Zugriff nach den verbleibenden Aufbewahrungstagen des Objekts	Numerischer Wert
s3:object-lock-retain-until-date	Filtert den Zugriff nach Datum der Objektaufbewahrung	Datum
s3:prefix	Filtert den Zugriff nach Schlüsselnamenpräfix	Zeichenfolge
s3:signatureAge	Filtert den Zugriff nach dem Alter der Anforderungssignatur in Millisekunden	Numerischer Wert
s3:signatureversion	Filtert den Zugriff nach der Version von AWS Signature, die in der Anforderung verwendet wird	String
s3:versionid	Filtert den Zugriff nach bestimmten Objektversionen	String

Bedingungsschlüssel	Beschreibung	Typ
s3:x-amz-acl	Filtert den Zugriff nach vordefinierter ACL im - x-amz-acl Header der Anforderung	String
s3:x-amz-content-sha256	Filtert den Zugriff auf nicht signierte Inhalte in Ihrem Bucket	String
s3:x-amz-copy-source	Filtert den Zugriff nach Kopierquellen-Bucket, Präfix oder Objekt in den Kopierobjektanforderungen	String
s3:x-amz-grant-full-control	Filtert den Zugriff nach x-amz-grant-full-Control-Header (vollständige Kontrolle)	String
s3:x-amz-grant-read	Filtert den Zugriff nach x-amz-grant-read (Lesezugriff)-Header	String
s3:x-amz-grant-read-acp	Filtert den Zugriff nach dem Header x-amz-grant-read-acp (Leseberechtigungen für die ACL)	String
s3:x-amz-grant-write	Filtert den Zugriff nach dem Header x-amz-grant-write (Schreibzugriff)	String
s3:x-amz-grant-write-acp	Filtert den Zugriff nach dem Header x-amz-grant-write-acp (Schreibberechtigungen für die ACL)	String
s3:x-amz-metadata-directive	Filtert den Zugriff nach Objekt-Metadatenverhalten (COPY oder REPLACE) beim Kopieren von Objekten	String
s3:x-amz-object-ownership	Filtert den Zugriff nach Objektbesitz	String
s3:x-amz-server-side-encryption	Filtert den Zugriff nach serverseitiger Verschlüsselung	String

Bedingungsschlüssel	Beschreibung	Typ
s3:x-amz-server-side-encryption-aws-kms-key-id	Filtert den Zugriff nach vom Kunden verwaltetem AWS KMS-CMK für die serverseitige Verschlüsselung	ARN
s3:x-amz-server-side-encryption-customer-algorithm	Filtert den Zugriff nach vom Kunden angegebenen Algorithmus für die serverseitige Verschlüsselung	String
s3:x-amz-storage-class	Filtert den Zugriff nach Speicherklasse	Zeichenfolge
s3:x-amz-website-redirect-location	Filtert den Zugriff nach bestimmten Websiteumleitungsorten für Buckets, die als statische Websites konfiguriert sind	String

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon S3 Express

Amazon S3 Express (Servicepräfix: `s3express`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon S3 Express definierte Aktionen
- Von Amazon S3 Express definierte Ressourcentypen

- Bedingungsschlüssel für Amazon S3 Express

Von Amazon S3 Express definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateBucket	Gewährt die Berechtigung zum Erstellen eines neuen Buckets.	Schreiben	bucket*		
				s3express:authType s3express:LocationName s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
CreateSession	Gewährt die Berechtigung zum Erstellen eines Sitzungstoken, das für Objekt-APIs wie PutObject, GetObject usw. verwendet wird	Lesen	bucket*		
				s3express:authType s3express:ResourceAccount	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3express:SessionMode s3express:signatureAge s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
DeleteBucket	Gewährt die Berechtigung zum Löschen des im URI benannten Buckets	Write	bucket*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
DeleteBucketPolicy	Gewährt die Berechtigung zum Löschen der Richtlinie für einen angegebenen Bucket	Berechtigungsverwaltung	bucket*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
GetBucketPolicy	Gewährt die Berechtigung zum Zurückgeben der Richtlinie des angegebenen Buckets	Lesen	bucket*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAllMyDirectoryBuckets	Gewährt die Berechtigung zum Auflisten aller Directory-Buckets, die dem authentifizierten Sender der Anforderung gehören.	Auflisten		s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutBucketPolicy	Gewährt die Berechtigung zum Hinzufügen oder Ersetzen einer Bucket-Richtlinie für einen Bucket	Berechtigungsverwaltung	bucket*	s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Von Amazon S3 Express definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
bucket	`arn:${Partition}:s3express:${Region}:${Account}:bucket/${BucketName}`	

Bedingungsschlüssel für Amazon S3 Express

Amazon S3 Express definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
s3express:LocationName	Filtert den Zugriff nach bestimmten Availability Zone-IDs	Zeichenfolge
s3express:ResourceAccount	Filtert den Zugriff nach der AWS-Konto-ID des Ressourcen-Eigentümers	Zeichenfolge
s3express:SessionMode	Filtert den Zugriff nach der von der CreateSession-API angeforderten Berechtigung, z. B. ReadOnly und ReadWrite	Zeichenfolge
s3express:TlsVersion	Filtert den Zugriff nach der TLS-Version, die vom Client verwendet wird	Numerischer Wert
s3express:authType	Filtert den Zugriff nach Authentifizierungsmethode	Zeichenfolge
s3express:signatureAge	Filtert den Zugriff nach dem Alter der Anforderungssignatur in Millisekunden	Numerischer Wert

Bedingungsschlüssel	Beschreibung	Typ
s3express:signatureversion	Filtert den Zugriff nach der Version von AWS-Signature, die für die Anforderung verwendet wird	Zeichenfolge
s3express:x-amz-content-sha256	Filtert den Zugriff auf nicht signierte Inhalte in Ihrem Bucket	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon S3 Glacier

Amazon S3 Glacier (Servicepräfix: `glacier`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon S3 Glacier definierte Aktionen
- Von Amazon S3 Glacier definierte Ressourcentypen
- Bedingungsschlüssel für Amazon S3 Glacier

Von Amazon S3 Glacier definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AbortMultipartUpload	Gewährt die Berechtigung zum Abbrechen eines mehrteiligen Upload, der durch die Upload-ID identifiziert ist.	Schreiben	vault*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AbortVaultLock	Gewährt die Berechtigung zum Abbrechen des Prozesses zum Sperren des Vaults, wenn die Vault Lock nicht den Status „Gesperrt“ aufweist.	Berechtigungsverwaltung	vault*		
AddTagsToVault	Gewährt die Berechtigung zum Hinzufügen von Tags zu einem Vault.	Markierung	vault*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CompleteMultipartUpload	Gewährt die Berechtigung zum Abschließen eines mehrteiligen Upload-Prozesses.	Schreiben	vault*		
CompleteVaultLock	Gewährt die Berechtigung zum Abschließen des Vault-Lock-Prozesses.	Berechtigungsverwaltung	vault*		
CreateVault	Gewährt die Berechtigung zum Erstellen eines neuen Vaults mit dem angegebenen Namen.	Schreiben	vault*		
DeleteArchive	Gewährt die Berechtigung zum Löschen eines Archivs aus einem Vault.	Schreiben	vault*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				glacier:ArchiveAgeInDays	
DeleteVault	Gewährt die Berechtigung zum Löschen eines Vaults.	Schreiben	vault*		
DeleteVaultAccessPolicy	Gewährt die Berechtigung zum Löschen der dem angegebenen Vault zugeordneten Zugriffsrichtlinie.	Berechtigungsverwaltung	vault*		
DeleteVaultNotifications	Gewährt die Berechtigung zum Löschen der für ein Vault eingestellten Benachrichtigungskonfiguration.	Schreiben	vault*		
DescribeJob	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Auftrag, der zuvor initiiert wurde,	Lesen	vault*		
DescribeVault	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Vault.	Lesen	vault*		
GetDataRetrievalPolicy	Gewährt die Berechtigung zum Abrufen der Datenabrufrichtlinie.	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetJobOutput	Gewährt die Berechtigung zum Herunterladen der Ausgabe des angegebenen Auftrags.	Lesen	vault*		
GetVaultAccessPolicy	Gewährt die Berechtigung zum Abrufen der im Vault festgelegten Zugriffsrichtlinie-Subressource.	Lesen	vault*		
GetVaultLock	Gewährt die Berechtigung zum Abrufen der Attribute aus der für das Vault festgelegten Sperrrichtlinie-Subressource.	Lesen	vault*		
GetVaultNotifications	Gewährt die Berechtigung zum Abrufen der im Vault festgelegten Benachrichtigungskonfiguration-Subressource.	Lesen	vault*		
InitiateJob	Gewährt die Berechtigung zum Initiieren eines Auftrags des angegebenen Typs.	Schreiben	vault*		
				glacier:ArchiveAgeInDays	
InitiateMultipartUpload	Gewährt die Berechtigung zum Initiieren eines mehrteiligen Uploads.	Schreiben	vault*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
InitiateVaultLock	Gewährt die Berechtigung zum Initiieren des Vault-Lock-Prozesses.	Berechtigungsverwaltung	vault*		
ListJobs	Gewährt die Berechtigung zum Auflisten der Aufträge für ein Vault sowie der kürzlich beendeten Aufträge.	Auflisten	vault*		
ListMultipartUploads	Gewährt die Berechtigung zum Auflisten der aktuell ausgeführten mehrteiligen Uploads für das angegebenen Vault.	Auflisten	vault*		
ListParts	Gewährt die Berechtigung zum Auflisten der Teile eines Archivs, die in einem bestimmten mehrteiligen Upload hochgeladen wurden.	Auflisten	vault*		
ListProvisionedCapacity	Gewährt die Berechtigung zum Auflisten der bereitgestellten Kapazität für das angegebene AWS-Konto.	Auflisten			
ListTagsForVault	Gewährt die Berechtigung zum Auflisten aller Tags, die einem Vault angefügt sind.	Auflisten	vault*		
ListVaults	Gewährt die Berechtigung zum Auflisten aller Vaults.	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PurchaseProvisionedCapacity	Gewährt die Berechtigung zum Kauf einer bereitgestellten Kapazitätseinheit für ein AWS-Konto.	Schreiben			
RemoveTagsFromVault	Gewährt die Berechtigung zum Entfernen eines oder mehrerer derjenigen Tags, die einem Vault angefügt sind.	Markierung	vault*		
SetDataRetrievalPolicy	Gewährt die Berechtigung zum Festlegen einer Richtlinie für den Datenabruf in der mit der PUT-Anforderung angegebenen Region und setzt diese durch.	Berechtigungsverwaltung			
SetVaultAccessPolicy	Gewährt die Berechtigung zum Hinzufügen einer Zugriffsichtlinie für ein Vault, überschreibt eine bereits vorhandene Richtlinie.	Berechtigungsverwaltung	vault*		
SetVaultNotifications	Gewährt die Berechtigung zum Konfigurieren von Vault-Benachrichtigungen.	Schreiben	vault*		
UploadArchive	Gewährt die Berechtigung zum Hochladen eines Archivs in ein Vault.	Schreiben	vault*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UploadMultipartPart	Gewährt die Berechtigung zum Hochladen eines Teils eines Archivs.	Schreiben	vault*		

Von Amazon S3 Glacier definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
vault	`arn:${Partition}:glacier:${Region}:${Account}:vaults/${VaultName}`	

Bedingungsschlüssel für Amazon S3 Glacier

Amazon S3 Glacier definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString
glacier:ArchiveAgeInDays	Filtert den Zugriff nach der Speicherdauer eines im Vault gespeicherten Archivs in Tagen.	Zeichenfolge
glacier:ResourceTag/	Filtert den Zugriff nach kundendefiniertem Tag.	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon S3 Object Lambda

Amazon S3 Object Lambda (Servicepräfix: `s3-object-lambda`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Aktionen, die von Amazon S3 Object Lambda definiert werden
- Von Amazon S3 Object Lambda definierte Ressourcentypen
- Bedingungsschlüssel für Amazon S3 Object Lambda

Aktionen, die von Amazon S3 Object Lambda definiert werden

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AbortMultipartUpload	Gewährt die Berechtigung zum Abbrechen eines mehrteiligen Uploads	Write	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
DeleteObject	Gewährt die Berechtigung zum Entfernen der Null-Version eines Objekts und zum Einfügen einer Löschmarkierung, die zur aktuellen Version des Objekts wird.	Write	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:s	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ignatureAge s3-object-lambda:TlsVersion	
DeleteObjectTagging	Gewährt die Berechtigung zum Verwenden der Tagging-Unterquelle, um den gesamten Tag-Satz aus dem angegebenen Objekt zu entfernen.	Markieren	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
DeleteObjectVersion	Gewährt die Berechtigung zum Entfernen einer bestimmten Version eines Objekts	Write	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
DeleteObjectVersionTagging	Erteilt die Berechtigung zum Entfernen des gesamten Tag-Satzes für eine bestimmte Version des Objekts	Markieren	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
GetObject	Gewährt die Berechtigung zum Abrufen von Objekten aus Amazon S3	Read	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectAcl	Gewährt die Berechtigung zum Zurückgeben der Zugriffskontrollliste (Access Control List, ACL) eines Objekts	Read	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectLegalHold	Gewährt die Berechtigung zum Abrufen des aktuellen „Legal Hold“-Status eines Objekts	Read	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectRetention	Gewährt die Berechtigung zum Abrufen der Aufbewahrungseinstellungen für ein Objekt	Read	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectTagging	Erteilt die Berechtigung zum Zurückgeben des Tag-Satzes eines Objekts	Read	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectVersion	Gewährt die Berechtigung zum Abrufen einer bestimmten Version eines Objekts	Read	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
GetObjectVersionAcl	Gewährt die Berechtigung zum Zurückgeben der Zugriffskontrollliste (Access Control List, ACL) einer bestimmten Objektversion	Read	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
GetObjectVersionTagging	Erteilt die Berechtigung zum Zurückgeben des Tag-Satzes für eine bestimmte Version des Objekts	Read	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
ListBucket	Gewährt die Berechtigung zum Auflisten einiger oder aller Objekte in einem Amazon-S3-Bucket (bis zu 1000)	List	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
ListBucketMultipartUploads	Gewährt die Berechtigung zum Auflisten in Bearbeitung befindlicher mehrteilige Uploads	List	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
ListBucketVersions	Erteilt die Berechtigung zum Auflisten von Metadaten zu allen Versionen von Objekten in einem Amazon-S3-Bucket	List	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
ListMultipartUploadParts	Gewährt die Berechtigung zum Auflisten der Teile, die für einen bestimmten mehrteiligen Upload hochgeladen wurden	List	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObject	Gewährt die Berechtigung zum Hinzufügen eines Objekts zu einem Bucket	Schreiben	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutObjectAcl	Gewährt die Berechtigung zum Festlegen der Berechtigungen für Zugriffskontrolllisten (Access Control Lists, ACL) für neue oder vorhandene Objekte in einem S3 Bucket	Berechtigungsverwaltung	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectLegalHold	Gewährt die Berechtigung zum Anwenden einer Legal Hold Konfiguration auf das angegebene Objekt	Write	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectRetention	Gewährt die Berechtigung zum Platzieren einer Objektaufbewahrungskonfiguration auf einem Objekt	Write	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectTagging	Erteilt die Berechtigung zum Festlegen des bereitgestellten Tag-Satzes für ein Objekt, das bereits in einem Bucket vorhanden ist	Markieren	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutObjectVersionAcl	Erteilt die Berechtigung zum Verwenden der ACL (Access Control List)-Unterquelle zum Festlegen der Access-Control-List-Berechtigungen für ein Objekt, das bereits in einem Bucket vorhanden ist	Permissions management	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
PutObjectVersionTagging	Erteilt die Berechtigung zum Festlegen des bereitgestellten Tag-Satzes für eine bestimmte Version eines Objekts	Markieren	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
RestoreObject	Gewährt die Berechtigung zum Wiederherstellen einer archivierten Kopie eines Objekts in Amazon S3	Write	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
WriteGetObjectResponse	Gewährt die Berechtigung zur Bereitstellung von Daten für GetObject-Anfragen, die an S3 Objekt Lambda gesendet werden	Write	objectlambdaaccesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	

Von Amazon S3 Object Lambda definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
objectlambdaaccesspoint	`arn:${Partition}:s3-object-lambda:${Region}:${Account}:accesspoint/${AccessPointName}`	

Bedingungsschlüssel für Amazon S3 Object Lambda

Amazon S3 Object Lambda definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
s3-object-lambda:TlsVersion	Filtert den Zugriff nach der TLS-Version, die vom Client verwendet wird	Numerischer Wert
s3-object-lambda:authType	Filtert den Zugriff nach Authentifizierungsmethode	Zeichenfolge
s3-object-lambda:signatureAge	Filtert den Zugriff nach dem Alter der Anforderungssignatur in Millisekunden	Numerischer Wert
s3-object-lambda:versionid	Filtert den Zugriff nach bestimmten Objektversionen	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon S3 in Outposts

Amazon S3 in Outposts (Servicepräfix: `s3-outposts`) stellen die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.

- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Aktionen, die von Amazon S3 in Outposts definiert werden
- Von Amazon S3 in Outposts definierte Ressourcentypen
- Bedingungsschlüssel für Amazon S3 in Outposts

Aktionen, die von Amazon S3 in Outposts definiert werden

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AbortMultipartUpload	Gewährt die Berechtigung zum Abbrechen eines mehrteiligen Uploads	Write	object*		
				s3-outposts:DataAccessPointArn s3-outposts:DataAccessPointAccount s3-outposts:AccessPointNetworkOrigin s3-outpos	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
CreateAccessPoint	Gewährt die Berechtigung zum Erstellen eines neuen Zugangspunkts	Write	accesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-outposts:x-amz-content-sha256	
CreateBucket	Gewährt die Berechtigung zum Erstellen eines neuen Buckets.	Write	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
CreateEndpoint	Gewährt die Berechtigung zum Erstellen eines neuen Endpunkts.	Write	endpoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteAccessPoint	Gewährt die Berechtigung zum Löschen des im URI benannten Zugriffspunkts	Write	accesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-outposts:DataAccessPointArn s3-outposts:DataAccessPointAccount s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-outposts:x-amz-content-sha256	
DeleteAccessPointPolicy	Gewährt die Berechtigung zum Löschen der Richtlinie auf einem angegebenen Zugriffspunkt	Berechtigungsverwaltung	accesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-outposts:DataAccessPointArn s3-outposts:DataAccessPointAccount s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-outposts:x-amz-content-sha256	
DeleteBucket	Gewährt die Berechtigung zum Löschen des im URI benannten Buckets	Write	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
DeleteBucketPolicy	Gewährt die Berechtigung zum Löschen der Richtlinie für einen angegebenen Bucket	Berechtigungsverwaltung	bucket*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
DeleteEndpoint	Gewährt die Berechtigung zum Löschen des im URI benannten Endpunkts	Write	endpoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteObject	Gewährt die Berechtigung zum Entfernen der Null-Version eines Objekts und zum Einfügen einer Löschmarkierung, die zur aktuellen Version des Objekts wird.	Write	object*		
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signat	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ureversion s3-outposts:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteObjectTagging	Gewährt die Berechtigung zum Verwenden der Tagging-Unterquelle, um den gesamten Tag-Satz aus dem angegebenen Objekt zu entfernen.	Markieren	object*		
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outpos	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteObjectVersion	Gewährt die Berechtigung zum Entfernen einer bestimmten Version eines Objekts	Write	object*		
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signat	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ureversion s3-outposts:versionid s3-outposts:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteObjectVersionTagging	Erteilt die Berechtigung zum Entfernen des gesamten Tag-Satzes für eine bestimmte Version des Objekts	Markierung	object*		
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outpos	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ts:signatureAge s3-outposts:signatureversion s3-outposts:versionid s3-outposts:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAccessPoint	Gewährt die Berechtigung zum Zurückgeben von Konfigurationsinformationen zum angegebenen Zugriffspunkt	Read		s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-outposts:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAccessPointPolicy	Gewährt die Berechtigung zum Zurückgeben der Zugriffspunktrichtlinie, die dem angegebenen Zugriffspunkt zugeordnet ist	Read	accesspoint*		
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outpos	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ts:signatureversion s3-outposts:x-amz-content-sha256	
GetBucket	Gewährt die Berechtigung zum Zurückgeben der Bucket-Konfiguration, die einem Amazon-S3-Bucket zugeordnet ist	Read	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBucketPolicy	Gewährt die Berechtigung zum Zurückgeben der Richtlinie des angegebenen Buckets	Read	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBucketTagging	Erteilt die Berechtigung zum Zurückgeben des Tag-Satzes, der einem Amazon-S3-Bucket zugeordnet ist	Read	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBucketVersioning	Erteilt die Berechtigung zum Zurückgeben des Versionssteuerungsstatus eines Amazon-S3-Buckets	Lesen	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetLifecycleConfiguration	Erteilt die Berechtigung zum Zurückgeben der Lebenszyklus-Konfigurationsinformationen, die in einem Amazon-S3-Bucket festgelegt sind.	Read	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
GetObject	Gewährt die Berechtigung zum Abrufen von Objekten aus Amazon S3	Read	object*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outposts:signatureAge	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
GetObjectTagging	Erteilt die Berechtigung zum Zurückgeben des Tag-Satzes eines Objekts	Read	object*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outposts:signatureAge	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
GetObjectVersion	Gewährt die Berechtigung zum Abrufen einer bestimmten Version eines Objekts	Lesen	object*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outposts:signatureAge	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-outposts:signatureversion s3-outposts:versionid s3-outposts:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetObjectVersionForReplication	Gewährt die Berechtigung, sowohl unverschlüsselte als auch mit SSE-KMS verschlüsselte Objekte zu replizieren	Lesen	object*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetObjectVersionTagging	Erteilt die Berechtigung zum Zurückgeben des Tag-Satzes für eine bestimmte Version des Objekts	Read	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outpos	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ts:signatureAge s3-outposts:signatureversion s3-outposts:versionid s3-outposts:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetReplicationConfiguration	Erteilt die Berechtigung zum Abrufen der in einem Amazon-S3-Bucket festgelegten Replikations-Konfigurationsinformationen	Lesen	bucket*	s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAccessPoints	Gewährt die Berechtigung zum Auflisten von Zugriffspunkten	List		s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
ListBucket	Erteilt die Berechtigung zum Auflisten einiger oder aller Objekte in einem Amazon-S3-Bucket (bis zu 1000)	List	accesspoint* bucket*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:delimiter s3-outposts:max-keys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-outposts:prefix s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
ListBucketMultipartUploads	Gewährt die Berechtigung zum Auflisten in Bearbeitung befindlicher mehrteilige Uploads	List	accesspoint* bucket*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-outposts:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListBucketVersions	Erteilt die Berechtigung zum Auflisten von Metadaten zu allen Versionen von Objekten in einem Amazon-S3-Bucket	Auflisten	bucket*		
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:delimiter s3-outpos	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ts:max-keys s3-outposts:prefix s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
ListEndpoints	Gewährt die Berechtigung zum Auflisten von Endpunkten	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListMultipartUploadParts	Gewährt die Berechtigung zum Auflisten der Teile, die für einen bestimmten mehrteiligen Upload hochgeladen wurden	Auflisten	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signat	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ureversion s3-outposts:x-amz-content-sha256	
ListOutpostsWithS3	Gewährt die Berechtigung zum Auflisten von Outposts mit S3-Kapazität	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListRegionalBuckets	Gewährt die Berechtigung zum Auflisten aller Buckets, die dem authentifizierten Sender der Anforderung gehören.	List		s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
ListSharedEndpoints	Gewährt die Berechtigung zum Auflisten von freigegebenen Endpunkten	Auflisten			
PutAccessPointPolicy	Gewährt die Berechtigung zum Zuordnen einer Zugriffsrichtlinie zu einem angegebenen Zugriffspunkt	Berechtigungsverwaltung	accesspoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-outposts:x-amz-content-sha256	
PutBucketPolicy	Gewährt die Berechtigung zum Hinzufügen oder Ersetzen einer Bucket-Richtlinie für einen Bucket	Berechtigungsverwaltung	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutBucketTagging	Gewährt die Berechtigung zum Hinzufügen eines Satzes von Tags zu einem vorhandenen Amazon-S3-Bucket	Markieren	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutBucketVersioning	Erteilt die Berechtigung zum Festlegen des Versionssteuerungsstatus eines vorhandenen Amazon-S3-Buckets	Schreiben	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutLifecycleConfiguration	Gewährt die Berechtigung zum Erstellen einer neuen Lebenszyklus-Konfiguration für den Bucket oder zum Ersetzen einer vorhandenen Lebenszyklus-Konfiguration	Write	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
PutObject	Gewährt die Berechtigung zum Hinzufügen eines Objekts zu einem Bucket	Write	object*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:RequestObjectTag/<key> s3-outposts:RequestObjectTagKeys s3-outpos	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-acl s3-outposts:x-amz-content-sha256 s3-outposts:x-amz-copy-source s3-outposts:x-amz-	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				metadata-directive s3-outposts:x-amz-server-side-encryption s3-outposts:x-amz-storage-class	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutObjectAcl	Gewährt die Berechtigung zum Festlegen der Zugriffskontrolllisten (ACL)-Berechtigungen für ein bereits in einem Bucket vorhandenes Objekt	Berechtigungsverwaltung	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outpos	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-acl s3-outposts:x-amz-content-sha256 s3-outposts:x-amz-storage-class	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutObjectTagging	Gewährt die Berechtigung zum Festlegen des bereitgestellten Tagsatzes für ein Objekt, das bereits in einem Bucket vorhanden ist	Markierung	object*		
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:RequestObjectTag/<key>	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-outposts:RequestObjectTagKeys s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutObjectVersionTagging	Erteilt die Berechtigung zum Festlegen des bereitgestellten Tag-Satzes für eine bestimmte Version eines Objekts	Markieren	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:RequestObjectTag/<key>	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				s3-outposts:RequestObjectTagKeys s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:versionid s3-outposts:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutReplicationConfiguration	Gewährt die Berechtigung zum Erstellen einer neuen Replikations-Konfiguration oder zum Ersetzen einer vorhandenen Replikations-Konfiguration	Schreiben	bucket*		iam:PassRole
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Replicate Delete	Gewährt die Berechtigung zum Replizieren von Löschmarkierungen auf den Ziel-Bucket	Write	object*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Replicate Object	Gewährt die Berechtigung zum Replizieren von Objekten und Objekt-Markierungen auf den Ziel-Bucket	Write	object*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256 s3-outposts:x-amz-server-side-encryption	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Replicate Tags	Gewährt die Berechtigung zum Replizieren von Objekt-Markierungen auf den Ziel-Bucket	Markierung	object*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Von Amazon S3 in Outposts definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
accesspoint	`arn:${Partition}:s3-outposts:${Region}:${Account}:outpost/${OutpostId}/accesspoint/${AccessPointName}`	
bucket	`arn:${Partition}:s3-outposts:${Region}:${Account}:outpost/${OutpostId}/bucket/${BucketName}`	
endpoint	`arn:${Partition}:s3-outposts:${Region}:${Account}:outpost/${OutpostId}/endpoint/${EndpointId}`	
object	`arn:${Partition}:s3-outposts:${Region}:${Account}:outpost/${OutpostId}/bucket/${BucketName}/object/${ObjectName}`	

Bedingungsschlüssel für Amazon S3 in Outposts

Amazon S3 in Outposts definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
s3-outposts:AccessPointNetworkOrigin	Filtert den Zugriff nach Netzwerkursprung (Internet oder VPC)	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
s3-outposts:DataAccessPointAccount	Filtert den Zugriff nach der AWS-Konto-ID, die Eigentümer des Zugriffspunkts ist	Zeichenfolge
s3-outposts:DataAccessPointArn	Filtert den Zugriff nach Amazon-Ressourcenname (ARN) des Zugriffspunkts	ARN
s3-outposts:ExistingObjectTag/<key>	Filtert den Zugriff durch die Anforderung, dass ein vorhandenes Objekt-Tag über einen bestimmten Tag-Schlüssel und -Wert verfügt	Zeichenfolge
s3-outposts:RequestObjectTag/<key>	Filtert den Zugriff durch Einschränkung der für Objekte zulässigen Tag-Schlüssel und -Werte	Zeichenfolge
s3-outposts:RequestObjectTagKeys	Filtert den Zugriff durch Einschränkung der für Objekte zulässigen Tag-Schlüssel	Zeichenfolge
s3-outposts:authType	Filtert den Zugriff durch Einschränkung der eingehenden Anfragen auf eine bestimmte Authentifizierungsmethode	Zeichenfolge
s3-outposts:delimiter	Filtert den Zugriff durch Anforderung von Parameter-Trennzeichen	Zeichenfolge
s3-outposts:max-keys	Filtert den Zugriff durch Begrenzung der maximalen Anzahl von Schlüsseln, die in einer ListBucket-Anforderung zurückgegeben werden	Numerischer Wert
s3-outposts:prefix	Filtert den Zugriff nach Schlüsselnamenpräfix	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
s3-outposts:signatureAge	Filtert den Zugriff durch die Identifizierung der Länge der Zeit in Millisekunden, für die eine Signatur in einer authentifizierten Anforderung gültig ist	Numerischer Wert
s3-outposts:signatureversion	Filtert den Zugriff durch die Identifizierung der Version von AWS Signature, die für authentifizierte Anforderungen unterstützt wird	Zeichenfolge
s3-outposts:versionid	Filtert den Zugriff nach bestimmten Objektversionen	Zeichenfolge
s3-outposts:x-amz-acl	Filtert den Zugriff durch Anforderung des x-amz-acl-Headers mit einer bestimmten zugeschnittenen ACL in einer Anforderung	Zeichenfolge
s3-outposts:x-amz-content-sha256	Filtert den Zugriff, indem nicht signierte Inhalte in Ihrem Bucket nicht zugelassen werden	Zeichenfolge
s3-outposts:x-amz-copy-source	Filtert den Zugriff durch Beschränkung der Kopierquelle auf einen bestimmten Bucket, Präfix oder ein bestimmtes Objekt	Zeichenfolge
s3-outposts:x-amz-metadata-directive	Filtert den Zugriff dadurch, das die Erzwingung des Verhaltens von Objektmetadaten (COPY oder REPLACE) beim Kopieren von Objekten ermöglicht wird	Zeichenfolge
s3-outposts:x-amz-server-side-encryption	Filtert den Zugriff durch Anforderung der serverseitigen Verschlüsselung	Zeichenfolge
s3-outposts:x-amz-storage-class	Filtert den Zugriff nach Speicherklasse	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon SageMaker

Amazon SageMaker (Service-Präfix:`sagemaker`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon definierte Aktionen SageMaker

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddAssociation	Erteilt die Erlaubnis, eine Abstammungseinheit (Artefakt, Kontext, Aktion, Experiment experiment-trial-component) miteinander zu verknüpfen	Schreiben	action*		
			artifact*		
			context*		
			experiment*		
			experiment-trial-component*		
AddTags	Erteilt die Erlaubnis, ein oder mehrere Tags für die	Tagging	action		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	angegebene SageMaker Amazon-Ressource hinzuzufügen oder zu überschreiben		algorithm		
			app		
			app-image-config		
			artifact		
			automl-job		
			cluster		
			code-repository		
			compilation-job		
			context		
			data-quality-job-definition		
			device		
			device-fleet		
			domain		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			edge-deployment-plan		
			edge-packaging-job		
			endpoint		
			endpoint-config		
			experiment		
			experiment-trial		
			experiment-trial-component		
			feature-group		
			flow-definition		
			human-task-ui		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			hyper-parameter-tuning-job		
			image		
			inference-component		
			inference-recommendations-job		
			labeling-job		
			model		
			model-bias-job-definition		
			model-card		
			model-explainability-job-definition		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			model-package		
			model-package-group		
			model-quality-job-definition		
			monitoring-schedule		
			notebook-instance		
			pipeline		
			processing-job		
			project		
			space		
			studio-lifecycle-config		
			training-job		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			transform-job		
			user-profile		
			workteam		
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:TaggingAction	
AssociateTrialComponent	Gewährt die Berechtigung zum Zuordnen einer Testkomponente	Schreiben	experiment-trial*		
			experiment-trial-component*		
BatchDescribeModelPackage	Erteilt die Erlaubnis, einen oder mehrere zu beschreiben ModelPackages	Lesen	model-package*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetMetrics [nur Berechtigung]	Erteilt die Berechtigung zum Abrufen von Metriken, die mit SageMaker Ressourcen wie Schulungsjobs oder Testkomponenten verknüpft sind. Diese API ist zu diesem Zeitpunkt nicht öffentlich zugreifbar, jedoch können Admins diese Aktion steuern	Lesen	experiment-trial-component*		
			training-job*		
BatchGetRecord	Gewährt die Berechtigung zum Abrufen eines Batch von Datensätzen aus einer oder mehreren Feature-Gruppen	Lesen	feature-group*		
BatchPutMetrics	Erteilt die Erlaubnis, Kennzahlen zu veröffentlichen, die mit einer SageMaker Ressource wie einer Schulung, einem Job oder einer Testkomponente verknüpft sind	Schreiben	experiment-trial-component*		
			training-job*		
CreateAction	Gewährt die Berechtigung zum Erstellen einer Aktion.	Schreiben	action*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAlgorithm	Gewährt die Berechtigung zum Erstellen eines Algorithmus.	Schreiben	algorithm*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateApp	Erteilt die Erlaubnis, eine App für einen SageMaker UserProfile oder Space zu erstellen	Schreiben	app*		sagemaker:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:ImageArns sagemaker:ImageVersionArns sagemaker:OwnerUserProfileArn sagemaker:SpaceSharingType	
CreateAppImageConfig	Erteilt die Erlaubnis zum Erstellen eines AppImageConfig	Schreiben	app-image-config*		sagemaker:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateArtifact	Gewährt die Berechtigung zum Erstellen eines Artifacts.	Schreiben	artifact*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAutoMLJob	Gewährt die Berechtigung zum Erstellen eines AutoML-Auftrags.	Schreiben	automl-job*		iam:PassRole sagemaker:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InterContainerTrafficEncryption sagemaker:OutputKmsKey sagemaker:VolumeKmsKey sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAutoMLJobV2	Gewährt die Berechtigung zum Erstellen eines V2-AutoML-Auftrags	Schreiben	automl-job*		iam:PassRole sagemaker:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InterContainerTrafficEncryption sagemaker:OutputKmsKey sagemaker:VolumeKmsKey sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCluster	Erteilt die Berechtigung zum Erstellen eines SageMaker HyperPod Clusters	Schreiben	cluster*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCodeRepository	Erteilt die Erlaubnis zum Erstellen eines CodeRepository	Schreiben	code-repository*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCompilationJob	Gewährt die Berechtigung zum Erstellen eines Kompilierauftrags.	Schreiben	compilation-job*		iam:PassRole sagemaker:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateContext	Gewährt die Berechtigung zum Erstellen eines Kontextes.	Schreiben	context*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataQualityJobDefinition	Gewährt die Berechtigung zum Erstellen einer Aufgabendefinition für die Datenqualität.	Schreiben	data-quality-job-definition*		iam:PassRole sagemaker:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:InterContainerTrafficEncryption sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateDeviceFleet	Gewährt die Berechtigung zum Erstellen einer Geräteflotte	Schreiben	device-fleet*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDomain	Erteilt die Berechtigung zum Erstellen einer Domain für SageMaker Studio	Schreiben	domain*		iam:CreateServiceLinkedRole iam:PassRole sagemaker:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:AppNetworkAccessType sagemaker:InstanceTypes sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets sagemaker:DomainSharingOutputKmsKey sagemaker:VolumeKmsKey	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				sagemaker:ImageArns sagemaker:ImageVersionArns	
CreateEdgeDeploymentPlan	Erteilt die Berechtigung zum Erstellen eines Edge-Bereitstellungsplans	Schreiben	edge-deployment-plan*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEdgeDeploymentStage	Erteilt die Berechtigung zum Erstellen einer Edge-Bereitstellungsphase	Schreiben	edge-deployment-plan*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateEdgePackagingJob	Gewährt die Berechtigung zum Erstellen einer Edge-Verpackungsaufgabe	Schreiben	edge-packaging-job*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEndpoint	Gewährt die Berechtigung zum Erstellen eines Endpunkts mit der in der Anforderung angegebenen Endpunktkonfiguration	Schreiben	endpoint*		sagemaker:AddTags
			endpoint-config*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEndpointConfig	Erteilt die Erlaubnis, eine Endpunktkonfiguration zu erstellen, die mithilfe der SageMaker Amazon-Hosting-Services bereitgestellt werden kann	Schreiben	endpoint-config*		iam:PassRole sagemaker:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:AcceleratorTypes sagemaker:InstanceTypes sagemaker:ModelArn sagemaker:VolumeKmsKey sagemaker:ServerlessMaxConcurrency sagemaker:ServerlessMemorySize	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				sagemaker:NetworkIsolation sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateExperiment	Gewährt die Berechtigung zum Erstellen eines Experiments	Schreiben	experiment*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFeatureGroup	Gewährt die Berechtigung zum Erstellen einer Feature-Gruppe	Schreiben	feature-group*		iam:PassRole sagemaker:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:FeatureGroupOnlineStoreKmsKey sagemaker:FeatureGroupOfflineStoreKmsKey sagemaker:FeatureGroupOfflineStoreS3Uri sagemaker:FeatureGroupEnableOnlineStore sagemaker:FeatureG	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				roupOfflineStoreConfig sagemaker:FeatureGroupDisableGlueTableCreation	
CreateFlowDefinition	Gewährt die Berechtigung zum Erstellen einer Ablauf-Definition, die Einstellungen für einen menschlichen Workflow definiert.	Schreiben	flow-definition*		iam:PassRole sagemaker:AddTags
				sagemaker:WorkteamArn sagemaker:WorkteamType aws:RequestTag/${TagKey} aws:TagKeys	
CreateHub	Gewährt die Berechtigung zum Erstellen eines Hubs	Schreiben	hub*		sagemaker:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHumanTaskUi	Gewährt die Berechtigung zum Definieren der Einstellungen, die für die Benutzeroberfläche des menschlichen Review-Workflows verwendet werden.	Schreiben	human-task-ui*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHyperParameterTuningJob	Erteilt die Erlaubnis, einen Hyperparameter-Tuning-Job zu erstellen, der mit Amazon bereitgestellt werden kann SageMaker	Schreiben	hyper-parameter-tuning-job*		iam:PassRole sagemaker:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:FileSystemAccessMode sagemaker:FileSystemDirectoryPath sagemaker:FileSystemId sagemaker:FileSystemType sagemaker:InstanceTypes sagemaker:InterContainerTrafficEncryption	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateImage	Erteilt die Erlaubnis, ein SageMaker Image zu erstellen	Schreiben	image*		iam:PassRole sagemaker:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateImageVersion	Erteilt die Erlaubnis zum Erstellen eines SageMaker ImageVersion	Schreiben	image*		
CreateInferenceComponent	Gewährt die Berechtigung zum Erstellen einer Inferenzkomponente auf einem Endpunkt	Schreiben	endpoint*		sagemaker:AddTags
			inference-component*		
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:ModelArn	
CreateInferenceExperiment	Gewährt die Berechtigung zum Erstellen eines Inferenzexperiments	Schreiben	inference-experiment*		iam:PassRole sagemaker:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInferenceRecommendationsJob	Gewährt die Berechtigung zum Erstellen eines Auftrags für Inferenzempfehlungen	Schreiben	inference-recommendations-job*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateLabelingJob	Gewährt Berechtigungen zum Starten eines Beschriftungsauftrags. Ein Labeling-Job nimmt unbeschriftete Daten auf und erzeugt beschriftete Daten als Ausgabe, die für SageMaker Trainingsmodelle verwendet werden können	Schreiben	labeling-job*		iam:PassRole sagemaker:AddTags
				sagemaker:WorkteamArn sagemaker:WorkteamType sagemaker:VolumeKmsKey sagemaker:OutputKmsKey aws:RequestTag/${TagKey} aws:TagKeys	
CreateLineageGroupPolicy	Gewährt die Berechtigung zum Erstellen einer Herkunftsgruppen-Richtlinie	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateModel	Erteilt die Erlaubnis, ein Modell in Amazon zu erstellen SageMaker. In der Anforderung geben Sie einen Namen für das Modell an und beschreiben mindestens einen Container.	Schreiben	model*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:NetworkIsolation sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateModelBiasJobDefinition	Gewährt die Berechtigung zum Erstellen einer Muster-Bias-Job-Definition	Schreiben	model-bias-job-definition*		iam:PassRole sagemaker:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:InterContainerTrafficEncryption sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateModelCard	Gewährt die Berechtigung zum Erstellen einer Modellkarte	Schreiben	model-card*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelCardExportJob	Gewährt die Berechtigung zum Erstellen eines Exportauftrags für eine Modellkarte	Schreiben	model-card*		
CreateModelExplainabilityJobDefinition	Gewährt die Berechtigung zum Erstellen einer Aufgabendefinition für die Erklärbarkeit eines Modells.	Schreiben	model-explainability-job-definition*		iam:PassRole sagemaker:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:InterContainerTrafficEncryption sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateModelPackage	Erteilt die Erlaubnis zum Erstellen eines ModelPackage	Schreiben	model-package		sagemaker:AddTags
			model-package-group		
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:ModelApprovalStatus sagemaker:CustomerMetadataProperties/${MetadataKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateModelPackageGroup	Erteilt die Erlaubnis zum Erstellen eines ModelPackageGroup	Schreiben	model-package-group*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelQualityJobDefinition	Gewährt die Berechtigung zum Erstellen einer Aufgabendefinition für die Modellqualität.	Schreiben	model-quality-job-definition*		iam:PassRole sagemaker:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:InterContainerTrafficEncryption sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateMonitoringSchedule	Gewährt die Berechtigung zum Erstellen eines Überwachungszeitplans.	Schreiben	monitoring-schedule*		iam:PassRole sagemaker:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:InterContainerTrafficEncryption sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateNotebookInstance	Erteilt die Erlaubnis, eine SageMaker Amazon-Notebook-Instance zu erstellen. Eine Notebook-Instance ist eine auf einem Jupyter-Notebook ausgeführte Amazon-EC2-Instance.	Schreiben	notebook-instance*		iam:PassRole sagemaker:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:AcceleratorTypes sagemaker:DirectInternetAccess sagemaker:InstanceTypes sagemaker:MinimumInstanceMetadataServiceVersion sagemaker:RootAccess sagemaker:VolumeKmsKey	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateNotebookInstanceLifecycleConfig	Erteilt die Erlaubnis, eine Lebenszykluskonfiguration für Notebook-Instances zu erstellen, die mit Amazon bereitgestellt werden kann SageMaker	Schreiben	notebook-instance-lifecycle-config*		
CreatePipeline	Gewährt die Berechtigung zum Erstellen einer Pipeline	Schreiben	pipeline*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreatePresignedDomainUrl	Erteilt die Erlaubnis, eine URL zurückzugeben, die Sie in Ihrem Browser verwenden können, um eine Verbindung zur Domain herzustellen, und zwar zu einem bestimmten UserProfile Zeitpunkt, wenn AuthMode es sich um „IAM“ handelt	Schreiben	user-profile*		
CreatePresignedNotebookInstanceUrl	Gewährt die Berechtigung zum Erstellen einer URL, die Sie im Browser verwenden können, um eine Verbindung zur Notebook-Instance herzustellen	Schreiben	notebook-instance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateProcessingJob	Gewährt die Berechtigung zum Starten eines Verarbeitungsauftrags Nach Abschluss der Verarbeitung SageMaker speichert Amazon die resultierenden Artefakte und andere optionale Ausgaben an einem von Ihnen angegebenen Amazon S3 S3-Speicherort.	Schreiben	processing-job*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets sagemaker:InterContainerTrafficEncryption	
CreateProject	Gewährt die Berechtigung zum Erstellen eines Projekts.	Schreiben	project*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSharedModel [nur Berechtigung]	Erteilt die Erlaubnis, ein gemeinsam genutztes Modell in einer SageMaker Studio-Anwendung zu erstellen	Schreiben	shared-model*		
CreateSpace	Erteilt die Erlaubnis, einen Space für eine SageMaker Domain zu erstellen	Schreiben	space*		sagemaker:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:ImageArns sagemaker:ImageVersionArns sagemaker:OwnerUserProfileArn sagemaker:SpaceSharingType	
CreateStudioLifecycleConfig	Erteilt die Erlaubnis, eine Studio Lifecycle-Konfiguration zu erstellen, die mit Amazon bereitgestellt werden kann SageMaker	Schreiben	studio-lifecycle-config*		sagemaker:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTrainingJob	Gewährt die Berechtigung zum Starten eines Trainingsauftrags. Nach Abschluss des Trainings SageMaker speichert Amazon die resultierenden Modellartefakte und andere optionale Ausgaben an einem von Ihnen angegebenen Amazon S3 S3-Speicherort.	Schreiben	training-job*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:FileSystemAccessMode sagemaker:FileSystemDirectoryPath sagemaker:FileSystemId sagemaker:FileSystemType sagemaker:InstanceTypes	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				sagemaker:InterContainerTrafficEncryption sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				sagemaker:KeepAlivePeriod sagemaker:EnableRemoteDebug	
CreateTransformJob	Gewährt die Berechtigung zum Starten eines Transformationsjobs Nachdem die Ergebnisse vorliegen, SageMaker speichert Amazon sie an einem von Ihnen angegebenen Amazon S3 S3-Speicherort	Schreiben	transform-job*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:ModelArn sagemaker:OutputKmsKey sagemaker:VolumeKmsKey	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTrial	Gewährt die Berechtigung zum Erstellen eines Tests	Schreiben	experiment*		sagemaker:AddTags
			experiment-trial*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTrialComponent	Gewährt die Berechtigung zum Erstellen einer Testkomponente	Schreiben	experiment-trial-component*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUserProfile	Erteilt die Erlaubnis, eine UserProfile für eine SageMaker Domain zu erstellen	Schreiben	user-profile*		iam:PassRole sagemaker:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:VpcSecurityGroupIds sagemaker:InstanceTypes sagemaker:DomainSharingOutputKmsKey sagemaker:ImageArns sagemaker:ImageVersionArns	
CreateWorkforce	Gewährt die Berechtigung zum Erstellen einer Belegschaft	Schreiben	workforce*		sagemaker:AddTags

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkteam	Gewährt die Berechtigung zum Erstellen einer neuen Arbeitsgruppe	Schreiben	workteam*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAction	Gewährt die Berechtigung zum Löschen einer Aktion.	Schreiben	action*		
DeleteAlgorithm	Gewährt die Berechtigung zum Löschen eines Algorithmus.	Schreiben	algorithm*		
DeleteApp	Gewährt die Berechtigung zum Löschen einer App	Schreiben	app*		
				sagemaker:OwnerUserProfileArn sagemaker:SpaceSharingType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteAppImageConfig	Erteilt die Erlaubnis zum Löschen eines AppImageConfig	Schreiben	app-image-config*		
DeleteArtifact	Gewährt die Berechtigung zum Löschen eines Artifacts.	Schreiben	artifact*		
DeleteAssociation	Erteilt die Erlaubnis, die Assoziation von einer Abstammungseinheit (Artefakt, Kontext, Aktion, Experiment experiment-trial-component) zu einer anderen zu löschen	Schreiben	action*		
			artifact*		
			context*		
			experiment*		
			experiment-trial-component*		
DeleteCluster	Erteilt die Berechtigung zum Löschen eines Clusters SageMaker HyperPod	Schreiben	cluster*		
DeleteCodeRepository	Erteilt die Erlaubnis zum Löschen eines CodeRepository	Schreiben	code-repository*		
DeleteCompilationJob	Gewährt die Berechtigung zum Löschen eines Kompilierungsauftrags	Schreiben	compilation-job*		
DeleteContext	Gewährt die Berechtigung zum Löschen eines Kontextes.	Schreiben	context*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteDataQualityJobDefinition	Erteilt die Berechtigung zum Löschen der mit der CreateDataQualityJobDefinition API erstellten Datenqualitäts-Auftragsdefinition	Schreiben	data-quality-job-definition*		
DeleteDeviceFleet	Gewährt die Berechtigung zum Löschen einer Geräteflotte	Schreiben	device-fleet*		
DeleteDomain	Gewährt die Berechtigung zum Löschen einer Domain	Schreiben	domain*		
DeleteEdgeDeploymentPlan	Erteilt die Berechtigung zum Löschen eines Edge-Bereitstellungsplans	Schreiben	edge-deployment-plan*		
DeleteEdgeDeploymentStage	Erteilt die Berechtigung zum Löschen einer Edge-Bereitstellungsphase	Schreiben	edge-deployment-plan*		
DeleteEndpoint	Gewährt die Berechtigung zum Löschen eines Endpunkts Amazon SageMaker gibt alle Ressourcen frei, die bei der Erstellung des Endpunkts bereitgestellt wurden	Schreiben	endpoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteEndpointConfig	Erteilt die Erlaubnis, die mit der CreateEndpointConfig API erstellte Endpunktkonfiguration zu löschen. Die DeleteEndpointConfig API löscht nur die angegebene Konfiguration. Sie löscht keine mit der Konfiguration erstellten Endpunkte.	Schreiben	endpoint-config*		
DeleteExperiment	Gewährt die Berechtigung zum Ausführen eines Experiments	Schreiben	experiment*		
DeleteFeatureGroup	Gewährt die Berechtigung zum Löschen einer Feature-Gruppe	Schreiben	feature-group*		
				aws:RequestTag/${TagKey}	
DeleteFlowDefinition	Gewährt die Berechtigung zum Löschen der angegebenen Flow-Definition	Schreiben	flow-definition*		
DeleteHub	Gewährt die Berechtigung zum Löschen von Hubs	Schreiben	hub*		
DeleteHubContent	Gewährt die Berechtigung zum Löschen von Hub-Inhalten	Schreiben	hub*		
			hub-content*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteHumanLoop	Gewährt die Berechtigung zum Löschen einer spezifizierten menschlichen Schleife	Schreiben	human-loop*		
DeleteHumanTaskUi	Gewährt die Berechtigung zum Löschen der angegebenen Benutzeroberfläche für menschliche Aufgaben (Worker-Task-Vorlage).	Schreiben	human-task-ui*		
DeleteHyperParameterTuningJob	Erteilt die Berechtigung zum Löschen eines Hyperparameter-Tuning-Jobs	Schreiben	hyper-parameter-tuning-job*		
DeleteImage	Erteilt die Berechtigung zum Löschen eines Images SageMaker	Schreiben	image*		
DeleteImageVersion	Erteilt die Erlaubnis zum Löschen eines SageMaker ImageVersion	Schreiben	image-version*		
DeleteInferenceComponent	Gewährt die Berechtigung zum Löschen einer Inferenzkomponente. Amazon SageMaker gibt die Ressourcen frei, die bei der Erstellung der Inferenzkomponente reserviert waren	Schreiben	inference-component*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteInferenceExperiment	Gewährt die Berechtigung zum Löschen eines Inferenzexperiments	Schreiben	inference-experiment*		
DeleteLineageGroupPolicy	Gewährt die Berechtigung zum Löschen einer IAM-Richtlinie aus einer Herkunftsgruppen-Richtlinie	Schreiben			
DeleteModel	Erteilt die Erlaubnis, ein mit der API erstelltes Modell zu löschen. CreateModel Die DeleteModel API löscht nur den Modelleintrag in Amazon SageMaker , den Sie durch den Aufruf der CreateModel API erstellt haben. Es löscht keine Modell-Artifacts, keinen Inferenzcode und nicht die IAM-Rolle, die Sie beim Erstellen des Modells angegeben haben	Schreiben	model*		
DeleteModelBiasJobDefinition	Erteilt die Erlaubnis, die mit der API erstellte Model Bias-Jobdefinition zu löschen CreateModelBiasJobDefinition	Schreiben	model-bias-job-definition*		
DeleteModelCard	Gewährt die Berechtigung zum Löschen einer Modellkarte	Schreiben	model-card*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteModelExplainabilityJobDefinition	Erteilt die Berechtigung zum Löschen der mit der API erstellten Jobdefinition zur Modellerklärbarkeit CreateModelExplainabilityJobDefinition	Schreiben	model-explainability-job-definition*		
DeleteModelPackage	Erteilt die Erlaubnis zum Löschen eines ModelPackage	Schreiben	model-package*		
DeleteModelPackageGroup	Erteilt die Erlaubnis zum Löschen eines ModelPackageGroup	Schreiben	model-package-group*		
DeleteModelPackageGroupPolicy	Erteilt die Berechtigung zum Löschen einer ModelPackageGroup Richtlinie	Schreiben	model-package-group*		
DeleteModelQualityJobDefinition	Erteilt die Berechtigung zum Löschen der mit der CreateModelQualityJobDefinition API erstellten Jobdefinition in Modellqualität	Schreiben	model-quality-job-definition*		
DeleteMonitoringSchedule	Gewährt die Berechtigung zum Löschen eines Überwachungszeitplans.	Schreiben	monitoring-schedule*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteNotebookInstance	Erteilt die Erlaubnis, eine SageMaker Amazon-Notebook-Instance zu löschen. Bevor Sie eine Notebook-Instance löschen können, müssen Sie die StopNotebookInstance API aufrufen	Schreiben	notebook-instance*		
DeleteNotebookInstanceLifecycleConfig	Gewährt die Berechtigung zum Löschen einer Notebook-Instance	Schreiben	notebook-instance-lifecycle-config*		
DeletePipeline	Gewährt die Berechtigung zum Löschen einer Pipeline	Schreiben	pipeline*		
DeleteProject	Gewährt die Berechtigung zum Löschen eines Projekts	Schreiben	project*		
DeleteRecord	Gewährt die Berechtigung zum Löschen eines Datensatzes aus einer Feature-Gruppe	Schreiben	feature-group*		
DeleteResourcePolicy [nur Berechtigung]	Erteilt AWS Resource Access Manager die Berechtigung, eine Ressourcenrichtlinie für eine Ressource zu löschen, die kontoübergreifende gemeinsame Nutzung unterstützt SageMaker	Schreiben			
DeleteSpace	Gewährt die Berechtigung zum Löschen eines Bereichs	Schreiben	space*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				sagemaker:OwnerUserProfileArn sagemaker:SpaceSharingType	
DeleteStudioLifecycleConfig	Gewährt die Berechtigung zum Löschen einer Studio-Lebenszykluskonfiguration	Schreiben	studio-lifecycle-config*		
DeleteTags	Erteilt die Erlaubnis, den angegebenen Satz von Tags aus einer SageMaker Amazon-Ressource zu löschen	Tagging	action		
			algorithm		
			app		
			app-image-config		
			artifact		
			automl-job		
			cluster		
			code-repository		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			compilation-job		
			context		
			data-quality-job-definition		
			device		
			device-fleet		
			domain		
			edge-deployment-plan		
			edge-packaging-job		
			endpoint		
			endpoint-config		
			experiment		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			experiment-trial		
			experiment-trial-component		
			feature-group		
			flow-definition		
			human-task-ui		
			hyper-parameter-tuning-job		
			image		
			inference-component		
			inference-recommendations-job		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			labeling-job		
			model		
			model-bias-job-definition		
			model-card		
			model-explainability-job-definition		
			model-package		
			model-package-group		
			model-quality-job-definition		
			monitoring-schedule		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			notebook-instance		
			pipeline		
			processing-job		
			project		
			space		
			studio-lifecycle-config		
			training-job		
			transform-job		
			user-profile		
			workteam		
				aws:TagKeys	
DeleteTrial	Gewährt die Berechtigung zum Löschen eines Tests	Schreiben	experiment-trial*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteTrialComponent	Gewährt die Berechtigung zum Löschen einer Testkomponente	Schreiben	experiment-trial-component*		
DeleteUserProfile	Erteilt die Erlaubnis zum Löschen eines UserProfile	Schreiben	user-profile*		
DeleteWorkforce	Gewährt die Berechtigung zum Löschen einer Belegschaft	Schreiben	workforce*		
DeleteWorkteam	Gewährt die Berechtigung zum Löschen einer Arbeitsgruppe	Schreiben	workteam*		
DeregisterDevices	Gewährt die Berechtigung zum Aufheben der Registrierung einer Reihe von Geräten	Schreiben	device*		
DescribeAction	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Aktion.	Lesen	action*		
DescribeAlgorithm	Gewährt die Berechtigung zum Beschreiben eines Algorithmus	Lesen	algorithm*		
DescribeApp	Gewährt die Berechtigung zur Beschreibung einer App	Lesen	app*		
DescribeAppImageConfig	Erteilt die Erlaubnis zur Beschreibung eines AppImageConfig	Lesen	app-image-config*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeArtifact	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Artifact.	Lesen	artifact*		
DescribeAutoMLJob	Erteilt die Erlaubnis, einen AutoML-Job zu beschreiben, der über die CreateAutoMLJob-API erstellt wurde	Lesen	automl-job*		
DescribeAutoMLJobV2	Erteilt die Erlaubnis, einen AutoML-Job zu beschreiben, der über die CreateAutoMLJobv2-API erstellt wurde	Lesen	automl-job*		
DescribeCluster	Erteilt die Erlaubnis, Informationen über einen Cluster zurückzugeben SageMaker HyperPod	Lesen	cluster*		
DescribeClusterNode	Erteilt die Berechtigung, Informationen über einen SageMaker HyperPod Clusterknoten zurückzugeben	Lesen	cluster*		
DescribeCodeRepository	Erteilt die Erlaubnis zur Beschreibung eines CodeRepository	Lesen	code-repository*		
DescribeCompilationJob	Gewährt die Berechtigung zum Erteilen der Berechtigung zum Zurückgeben von Informationen über eine Transkriptionsaufgabe.	Lesen	compilation-job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeContext	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Kontext.	Lesen	context*		
DescribeDataQualityJobDefinition	Gewährt die Berechtigung, Informationen zu einer Aufgabendefinition für die Datenqualität zurückzugeben.	Lesen	data-quality-job-definition*		
DescribeDevice	Gewährt die Berechtigung, auf Informationen zu einem Gerät zuzugreifen	Lesen	device*		
DescribeDeviceFleet	Gewährt die Berechtigung, auf Informationen zu einer Geräteflotte zuzugreifen	Lesen	device-fleet*		
DescribeDomain	Gewährt die Berechtigung zur Beschreibung einer Domain	Lesen	domain*		
DescribeEdgeDeploymentPlan	Erteilt die Berechtigung zum Zugriff auf Informationen zu einem Edge-Bereitstellungsplan	Lesen	edge-deployment-plan*		
DescribeEdgePackagingJob	Gewährt die Berechtigung, auf Informationen zu einer Edge-Verpackungsaufgabe zuzugreifen	Lesen	edge-packaging-job*		
DescribeEndpoint	Gewährt die Berechtigung, die Beschreibung eines Endpunkts zurückzugeben	Lesen	endpoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeEndpointConfig	Erteilt die Erlaubnis, die Beschreibung einer Endpunktkonfiguration zurückzugeben, die mithilfe der CreateEndpointConfig API erstellt wurde	Lesen	endpoint-config*		
DescribeExperiment	Gewährt die Berechtigung zum Zurückgeben von Informationen zu einem Experiment	Lesen	experiment*		
DescribeFeatureGroup	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Feature-Gruppe	Lesen	feature-group*		
DescribeFeatureMetadata	Gewährt die Berechtigung zum Abrufen von Informationen zu Metadaten eines Features	Lesen	feature-group*		
DescribeFlowDefinition	Gewährt die Berechtigung zum Zurückgeben von Informationen zur angegebenen Flowdefinition	Lesen	flow-definition*		
DescribeHub	Gewährt die Berechtigung zum Beschreiben von Hubs	Lesen	hub*		
DescribeHubContent	Gewährt die Berechtigung zum Beschreiben eines Hub-Inhalts	Lesen	hub* hub-content*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeHumanLoop	Gewährt die Berechtigung zum Zurückgeben von Informationen zur angegebenen menschlichen Schleife	Lesen	human-loop*		
DescribeHumanTaskUi	Gewährt die Berechtigung, detaillierte Informationen über die angegebene Benutzeroberfläche für den menschlichen Review-Workflow zurückzugeben	Lesen	human-task-ui*		
DescribeHyperParameterTuningJob	Erteilt die Berechtigung zur Beschreibung eines Hyperparameter-Tuning-Jobs, der über die CreateHyperParameterTuningJob API erstellt wurde	Lesen	hyper-parameter-tuning-job*		
DescribeImage	Erteilt die Erlaubnis, Informationen über ein SageMaker Bild zurückzugeben	Lesen	image*		
DescribeImageVersion	Erteilt die Erlaubnis, Informationen über ein zurückzugeben SageMaker ImageVersion	Lesen	image-version*		
DescribeInferenceComponent	Gewährt die Berechtigung, die Beschreibung einer Inferenzkomponente zurückzugeben	Lesen	inference-component*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeInferenceExperiment	Gewährt die Berechtigung zum Abrufen von Informationen über ein Inferenzexperiment	Lesen	inference-experiment*		
DescribeInferenceRecommendationsJob	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Auftrag für Inferenzempfehlungen	Lesen	inference-recommendations-job*		
DescribeLabelingJob	Gewährt die Berechtigung zum Erteilen der Berechtigung zum Zurückgeben von Informationen zu einer Domain.	Lesen	labeling-job*		
DescribeLineageGroup	Gewährt die Berechtigung zum Beschreiben einer Herkunftsgruppe	Lesen			
DescribeModel	Erteilt die Erlaubnis, ein Modell zu beschreiben, das Sie mithilfe der CreateModel API erstellt haben	Lesen	model*		
DescribeModelBiasJobDefinition	Gewährt die Berechtigung, Informationen zu einer Aufgabendefinition für die Modellverzerrung zurückzugeben.	Lesen	model-bias-job-definition*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeModelCard	Gewährt die Berechtigung zum Abrufen von Informationen über eine Modellkarte	Lesen	model-card*		
DescribeModelCardExportJob	Gewährt die Berechtigung zum Abrufen von Informationen über einen Exportauftrag einer Modellkarte	Lesen	model-card-export-job*		
DescribeModelExplainabilityJobDefinition	Gewährt die Berechtigung, Informationen zu einer Aufgabendefinition für die Erklärbarkeit eines Modells zurückzugeben.	Lesen	model-explainability-job-definition*		
DescribeModelPackage	Erteilt die Erlaubnis zur Beschreibung eines ModelPackage	Lesen	model-package*		
DescribeModelPackageGroup	Erteilt die Erlaubnis zur Beschreibung eines ModelPackageGroup	Lesen	model-package-group*		
DescribeModelQualityJobDefinition	Gewährt die Berechtigung, Informationen zu einer Aufgabendefinition für die Modellqualität zurückzugeben.	Lesen	model-quality-job-definition*		
DescribeMonitoringSchedule	Gewährt die Berechtigung, Informationen zu einem Überwachungszeitplan zurückzugeben.	Lesen	monitoring-schedule*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeNotebookInstance	Gewährt die Berechtigung zum Abrufen von Informationen über eine Notebook-Instance	Lesen	notebook-instance*		
DescribeNotebookInstanceLifecycleConfig	Erteilt die Erlaubnis, eine Lebenszykluskonfiguration einer Notebook-Instanz zu beschreiben, die über die CreateNotebookInstanceLifecycleConfig API erstellt wurde	Lesen	notebook-instance-lifecycle-config*		
DescribePipeline	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Pipeline.	Lesen	pipeline*		
DescribePipelineDefinitionForExecution	Gewährt die Berechtigung zum Abrufen der Pipeline-Definition für eine Pipeline-Ausführung.	Lesen	pipeline-execution*		
DescribePipelineExecution	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Pipeline-Ausführung.	Lesen	pipeline-execution*		
DescribeProcessingJob	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Bearbeitungsauftrag	Lesen	processing-job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeProject	Gewährt die Berechtigung zum Beschreiben eines Projekts	Lesen	project*		
DescribeSharedModel [nur Berechtigung]	Erteilt die Berechtigung zur Beschreibung eines gemeinsam genutzten Modells in einer SageMaker Studio-Anwendung	Lesen	shared-model*		
DescribeSpace	Gewährt die Berechtigung zum Beschreiben eines Bereichs	Lesen	space*		
DescribeStudioLifecycleConfig	Gewährt die Berechtigung zum Beschreiben einer Studio-Lebenszykluskonfiguration	Lesen	studio-lifecycle-config*		
DescribeSubscribedWorkteam	Gewährt die Berechtigung zum Zurückgeben von Informationen zu einem abonnierten Arbeitsteam	Lesen	workteam*		
DescribeTrainingJob	Gewährt die Berechtigung zum Zurückgeben von Informationen über eine Trainingsaufgabe.	Lesen	training-job*		
DescribeTransformJob	Gewährt die Berechtigung zum Zurückgeben von Informationen über eine Transformationsaufgabe.	Lesen	transform-job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeTrial	Gewährt die Berechtigung zum Zurückgeben von Informationen zu einem Test.	Lesen	experiment-trial*		
DescribeTrialComponent	Gewährt die Berechtigung zum Zurückgeben von Informationen zu einem Testkomponenten.	Lesen	experiment-trial-component*		
DescribeUserProfile	Erteilt die Erlaubnis zur Beschreibung eines UserProfile	Lesen	user-profile*		
DescribeWorkforce	Gewährt die Berechtigung zum Zurückgeben von Informationen zu einer Belegschaft.	Lesen	workforce*		
DescribeWorkteam	Gewährt die Berechtigung zum Zurückgeben von Informationen zu einer Arbeitsgruppe.	Lesen	workteam*		
DisableSagemakerServicecatalogPortfolio	Erteilt die Berechtigung zur Deaktivierung eines SageMaker Servicekatalog-Portfolios	Schreiben			
DisassociateTrialComponent	Gewährt die Berechtigung, eine Testkomponente von einer Testversion zu trennen	Schreiben	experiment-trial*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			experiment-trial-component*		
			processing-job*		
EnableSagemakerServicecatalogPortfolio	Erteilt die Erlaubnis, ein SageMaker Servicekatalog-Portfolio zu aktivieren	Schreiben			
GetDeployments	Gewährt die Berechtigung zum Abrufen eines Bereitstellungsplans für das Gerät	Lesen	device*		
GetDeviceFleetReport	Gewährt die Berechtigung, auf eine Zusammenfassung der Geräte in einer Geräteflotte zuzugreifen	Lesen	device-fleet*		
GetDeviceRegistration	Gewährt die Berechtigung zum Abrufen der Geräteregistrierung. Nach der Bereitstellung eines Modells auf Edge-Geräten wird diese API verwendet, um die aktuelle Geräteregistrierung abzurufen.	Lesen	device*		
GetLineageGroupPolicy	Gewährt die Berechtigung zum Abrufen einer Herkunftsgruppen-Richtlinie	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetModelPackageGroupPolicy	Erteilt die Erlaubnis zum Abrufen einer ModelPackageGroup Richtlinie	Lesen	model-package-group*		
GetRecord	Gewährt die Berechtigung zum Abrufen eines Datensatzes aus einer Feature-Gruppe	Lesen	feature-group*		
GetResourcePolicy [nur Berechtigung]	Erteilt AWS Resource Access Manager die Berechtigung, eine Ressourcenrichtlinie für eine Ressource abzurufen, die kontenübergreifende gemeinsame Nutzung unterstützt SageMaker	Lesen			
GetSagemakerServicecatalogPortfolioStatus	Erteilt die Erlaubnis zum Abrufen eines SageMaker Servicekatalog-Portfolios	Lesen			
GetScalingConfigurationRecommendation	Gewährt die Berechtigung zum Abrufen einer Empfehlung zur Konfiguration der Skalierungsrichtlinie	Lesen	inference-recommendations-job*		
GetSearchSuggestions	Gewährt die Berechtigung zum Abrufen von Suchvorschlägen bei Angabe mit Schlüsselwort	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ImportHubContent	Gewährt die Berechtigung zum Importieren von Hub-Inhalten	Schreiben	hub*		sagemaker:AddTags
			hub-content*		
				aws:RequestTag/${TagKey} aws:TagKeys	
InvokeEndpoint	Gewährt die Berechtigung zum Aufrufen eines Endpunkts. Nachdem Sie ein Modell mithilfe von SageMaker Amazon-Hosting-Services in der Produktion bereitgestellt haben, verwenden Ihre Client-Anwendungen diese API, um Rückschlüsse aus dem Modell zu ziehen, das auf dem angegebenen Endpunkt gehostet wird.	Lesen	endpoint*		
			inference-component		
				sagemaker:TargetModel	
InvokeEndpointAsync	Gewährt die Berechtigung zum Abrufen von Schlussfolgerungen aus dem gehosteten Modell am angegebenen Endpunkt asynchron	Lesen	endpoint*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
InvokeEndpointWithResponseStream	Gewährt die Berechtigung zum Abrufen der Inferenzantwort als Stream vom angegebenen Endpunkt	Lesen	endpoint* inference-component		
ListActions	Gewährt die Berechtigung zum Auflisten von Aktionen.	List			
ListAlgorithms	Gewährt die Berechtigung zum Auflisten von Algorithmen.	Auflisten			
ListAliases	Erteilt die Erlaubnis, Aliase aufzulisten, die zu einem SageMaker Bild oder Sagemaker gehören ImageVersion	Auflisten	image* image-version*		
ListAppImageConfigs	Erteilt die Erlaubnis, sie in Ihrem Konto aufzulisten AppImageConfigs	Auflisten			
ListApps	Gewährt die Berechtigung zum Auflisten der Apps in Ihrem Konto	List			
ListArtifacts	Gewährt die Berechtigung zum Auflisten von Artifacts.	List			
ListAssociations	Gewährt die Berechtigung zum Auflisten von Mappings.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAutoMLJobs	Gewährt die Berechtigung zum Auflisten von AutoML-Aufträgen	List			
ListCandidatesForAutoMLJob	Gewährt die Berechtigung, Kandidaten für einen AutoML Job aufzulisten	Auflisten			
ListClusterNodes	Erteilt die Erlaubnis, Knoten innerhalb eines SageMaker HyperPod Clusters aufzulisten	Auflisten	cluster*		
ListClusters	Erteilt die Erlaubnis, SageMaker HyperPod Cluster aufzulisten	Auflisten			
ListCodeRepositories	Gewährt die Berechtigung zum Auflisten von Code-Repositorys.	List			
ListCompilationJobs	Gewährt die Berechtigung zum Auflisten von Kompilieraufträgen	Auflisten			
ListContexts	Gewährt die Berechtigung zum Auflisten von Kontexten	Auflisten			
ListDataQualityJobDefinitions	Gewährt die Berechtigung zum Auflisten von Aufgabendefinitionen für die Datenqualität.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDeviceFleets	Gewährt die Berechtigung zum Auflisten von Geräteflotten	List			
ListDevices	Gewährt die Berechtigung zum Auflisten von Geräten.	List			
ListDomains	Gewährt die Berechtigung zum Auflisten der Domains in Ihrem Konto	Auflisten			
ListEdgeDeploymentPlans	Gewährt die Berechtigung zum Auflisten von Edge-Bereitstellungsplänen	Auflisten			
ListEdgePackagingJobs	Gewährt die Berechtigung zum Auflisten von Edge-Verpackungsaufgaben	List			
ListEndpointConfigs	Gewährt die Berechtigung zum Auflisten von Endpunktkonfigurationen	List			
ListEndpoints	Gewährt die Berechtigung zum Auflisten von Endpunkten	List			
ListExperiments	Gewährt die Berechtigung, alle Experimente aufzulisten	List			
ListFeatureGroups	Gewährt die Berechtigung zum Auflisten von Feature-Gruppen	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListFlowDefinitions	Gewährt die Berechtigung zum Zurückgeben von zusammenfassenden Informationen über Ablauf-Definitionen für die angegebenen Parameter.	Auflisten			
ListHubContentVersions	Gewährt die Berechtigung zum Auflisten von allen Versionen des Hub-Inhalts	Auflisten	hub*		
			hub-content*		
ListHubContents	Gewährt die Berechtigung zum Auflisten der neuesten Versionen des Hub-Inhalts	Auflisten	hub*		
ListHubs	Gewährt die Berechtigung zum Auflisten von Hubs	Auflisten			
ListHumanLoops	Gewährt die Berechtigung zum Zurückgeben einer Zusammenfassung der Informationen über menschliche Schleifen für die angegebenen Parameter.	List			
ListHumanTaskUis	Gewährt die Berechtigung zum Zurückgeben einer Zusammenfassung der Benutzeroberflächen von menschlichen Review-Workflows für die angegebenen Parameter.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListHyperParameterTuningJobs	Gewährt die Berechtigung zum Auflisten von Hyperparametern-Einstellarbeiten	Auflisten			
ListImageVersions	Erteilt die Berechtigung, Listen aufzulisten ImageVersions , die zu einem SageMaker Image gehören	Auflisten	image*		
ListImages	Erteilt die Erlaubnis, SageMaker Bilder in Ihrem Konto aufzulisten	Auflisten			
ListInferenceComponents	Gewährt Berechtigung zum Auflisten von Inferenzkomponenten	Auflisten			
ListInferenceExperiments	Gewährt die Berechtigung zum Auflisten von allen Inferenzexperimenten	Auflisten			
ListInferenceRecommendationsJobSteps	Gewährt die Auflistung von Auftragsschritten für Inferenzempfehlungen	Auflisten			
ListInferenceRecommendationsJobs	Gewährt die Berechtigung zum Erstellen eines Auftrags für Inferenzempfehlungen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListLabelingJobs	Gewährt die Berechtigung zum Auflisten von Markierungsaufträgen	List			
ListLabelingJobsForWorkteam	Gewährt die Berechtigung zum Auflisten von Labelaufträgen für Arbeitsteam	Auflisten	workteam*		
ListLineageGroups	Gewährt die Berechtigung zum Auflisten von Herkunftsgruppen	Auflisten			
ListModelBiasJobDefinitions	Gewährt die Berechtigung zum Auflisten von Aufgabendefinitionen für die Modellverzerrung.	Auflisten			
ListModelCardExportJobs	Gewährt die Berechtigung zum Auflisten von Exportaufträgen für eine Modellkarte	Auflisten	model-card*		
ListModelCardVersions	Gewährt die Berechtigung zum Auflisten der Versionen einer Modellkarte	Auflisten	model-card*		
ListModelCards	Gewährt die Berechtigung zum Auflisten von Modellkarten	Auflisten			
ListModelExplainabilityJobDefinitions	Gewährt die Berechtigung zum Auflisten von Aufgabendefinitionen für die Erklärbarkeit eines Modells.	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListModelMetadata	Gewährt die Berechtigung zum Auflisten von Modellmetadaten für Aufträge für Inferenzempfehlungen	Auflisten			
ListModelPackageGroups	Erteilt die Erlaubnis zum Auflisten ModelPackageGroups	Auflisten			
ListModelPackages	Erteilt die Erlaubnis zum Auflisten ModelPackages	Auflisten	model-package		
ListModelQualityJobDefinitions	Gewährt die Berechtigung zum Auflisten von Aufgabendefinitionen für die Modellqualität.	Auflisten			
ListModels	Erteilt die Erlaubnis, die mit der CreateModel API erstellten Modelle aufzulisten	Auflisten			
ListMonitoringAlertHistory	Gewährt die Berechtigung zum Auflisten des Verlaufs einer Überwachungswarnung	Auflisten			
ListMonitoringAlerts	Gewährt die Berechtigung zum Auflisten von Überwachungswarnungen	Auflisten			
ListMonitoringExecutions	Gewährt die Berechtigung zum Auflisten von Überwachungsausführungen.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListMonitoringSchedules	Gewährt die Berechtigung zum Auflisten von Überwachungszeitplänen.	Auflisten			
ListNotebookInstanceLifecycleConfigs	Erteilt die Erlaubnis, die Lebenszykluskonfigurationen für Notebook-Instances aufzulisten, die mit Amazon bereitgestellt werden können SageMaker	Auflisten			
ListNotebookInstances	Erteilt die Erlaubnis, die SageMaker Amazon-Notebook-Instances im Konto des Anforderers in einem aufzulisten AWS-Region	Auflisten			
ListPipelineExecutionSteps	Gewährt die Berechtigung zum Auflisten von Schritten für eine Pipeline-Ausführung	List	pipeline-execution*		
ListPipelineExecutions	Gewährt die Berechtigung zum Auflisten von Ausführungen für eine Pipeline	List	pipeline*		
ListPipelineParametersForExecution	Gewährt die Berechtigung zum Auflisten von Parametern für eine Pipeline-Ausführung	List	pipeline-execution*		
ListPipelines	Gewährt die Berechtigung zum Auflisten von Pipelines.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListProcessingJobs	Gewährt die Berechtigung zum Auflisten von Bearbeitungsaufträge	List			
ListProjects	Gewährt die Berechtigung zum Auflisten von Projekten.	Auflisten			
ListResourceCatalogs	Gewährt die Berechtigung zum Auflisten von Ressourcenkatalogen	Auflisten			
ListSharedModelEvents [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von freigegebenen Modellereignissen	Auflisten			
ListSharedModelVersions [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der freigegebenen Versionen eines Modells	Auflisten	shared-model*		
ListSharedModels [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von freigegebenen Modellen	Auflisten			
ListSpaces	Gewährt die Berechtigung zum Auflisten der Bereiche in Ihrem Konto	Auflisten			
ListStageDevices	Gewährt die Berechtigung, Phasengeräte aufzulisten	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListStudioLifecycleConfigs	Erteilt die Erlaubnis, die Studio Lifecycle-Konfigurationen aufzulisten, die mit Amazon bereitgestellt werden können SageMaker	Auflisten			
ListSubscribedWorkteams	Gewährt die Berechtigung zum Auflisten abonnierter Arbeitsgruppen	List			
ListTags	Gewährt die Berechtigung zum Auflisten des Tag-Sets, das mit der angegebenen Ressource verknüpft ist	List	action		
			algorithm		
			app		
			app-image-config		
			artifact		
			automl-job		
			cluster		
			code-repository		
			compilation-job		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			context		
			data-quality-job-definition		
			device		
			device-fleet		
			domain		
			edge-deployment-plan		
			edge-packaging-job		
			endpoint		
			endpoint-config		
			experiment		
			experiment-trial		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			experiment-trial-component		
			feature-group		
			flow-definition		
			human-task-ui		
			hyper-parameter-tuning-job		
			image		
			inference-component		
			inference-recommendations-job		
			labeling-job		
			model		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			model-bias-job-definition		
			model-card		
			model-explainability-job-definition		
			model-package		
			model-package-group		
			model-quality-job-definition		
			monitoring-schedule		
			notebook-instance		
			pipeline		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			processing-job		
			project		
			space		
			studio-lifecycle-config		
			training-job		
			transform-job		
			user-profile		
			workteam		
ListTrainingJobs	Gewährt die Berechtigung zum Auflisten von Trainingaufträgen	List			
ListTrainingJobsForHyperParameterTuningJob	Gewährt die Berechtigung zum Auflisten von Trainingsaufträgen für einen Hyperparameter-Optimierungsauftrag	List	hyper-parameter-tuning-job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTransformJobs	Gewährt die Berechtigung zum Auflisten von Transformationsaufgaben	List			
ListTrialComponents	Gewährt Berechtigung zum Auflisten von Testkomponenten	List			
ListTrials	Gewährt die Berechtigung zum Auflisten von Tests	Auflisten			
ListUserProfiles	Erteilt die Erlaubnis, die UserProfiles in Ihrem Konto aufzulisten	Auflisten			
ListWorkforces	Gewährt die Berechtigung zum Auflisten von Mitarbeitern	List			
ListWorkteams	Gewährt die Berechtigung zum Auflisten von Arbeitsgruppen	Auflisten			
PutLineageGroupPolicy	Gewährt die Berechtigung zum Ablegen einer Herkunftsgruppen-Richtlinie	Schreiben			
PutModelPackageGroupPolicy	Erteilt die Erlaubnis, eine ModelPackageGroup Richtlinie zu erstellen	Schreiben	model-package-group*		
PutRecord	Gewährt die Berechtigung zum Ablegen eines Datensatzes in einer Feature-Gruppe	Schreiben	feature-group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutResourcePolicy [nur Berechtigung]	Erteilt AWS Resource Access Manager die Berechtigung, eine Ressourcenrichtlinie für eine Ressource zu erstellen , die die kontoübergreifende gemeinsame Nutzung unterstützt SageMaker	Schreiben			
QueryLineage	Gewährt die Berechtigung zum Untersuchen des Herkunftsdiagramms	Auflisten			
RegisterDevices	Gewährt die Berechtigung zum Registrieren einer Reihe von Geräten	Schreiben	device*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RenderUiTemplate	Gewährt die Berechtigung zur Darstellung einer UI-Vorlage für eine menschliche Anmerkungsaufgabe	Lesen			iam:PassRole
RetryPipelineExecution	Gewährt die Berechtigung zum Neustarten einer Pipeline-Ausführung	Schreiben	pipeline-execution*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Search	Erteilt die Berechtigung, nach Objekten zu suchen SageMaker	Lesen		sagemaker:SearchVisibilityCondition/${FilterKey}	
SendHeartbeat	Gewährt die Berechtigung, Heartbeat-Daten von Geräten zu veröffentlichen. Nachdem Sie ein Modell auf Edge-Geräten bereitgestellt haben, wird diese API verwendet, um den Gerätestatus zu melden	Schreiben	device*		
SendPipelineExecutionStepFailure	Gewährt die Berechtigung, einen ausstehenden Rückrufschritt fehlschlagen	Schreiben	pipeline-execution*		
SendPipelineExecutionStepSuccess	Gewährt die Berechtigung zum Erfolg eines ausstehenden Callback-Schritts	Schreiben	pipeline-execution*		
SendSharedModelEvent [nur Berechtigung]	Gewährt die Berechtigung zum Senden eines freigegebenen Modellereignis	Schreiben	shared-model-event*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartEdgeDeploymentStage	Erteilt die Berechtigung zum Starten einer Edge-Bereitstellungsphase	Schreiben	edge-deployment-plan*		
StartHumanLoop	Gewährt die Berechtigung zum Starten einer menschlichen Schleife	Schreiben	flow-definition*		
StartInferenceExperiment	Gewährt die Berechtigung zum Starten eines Inferenzexperiments	Schreiben	inference-experiment*		
StartMonitoringSchedule	Gewährt die Berechtigung zum Starten eines Überwachungszeitplans.	Schreiben	monitoring-schedule*		
StartNotebookInstance	Gewährt die Berechtigung zum Starten einer Notebook-Instance. Startet eine EC2 Instance mit der neuesten Version der Bibliotheken und fügt sie an das EBS-Volume an	Schreiben	notebook-instance*		
StartPipelineExecution	Gewährt die Berechtigung zum Starten einer Pipeline-Ausführung.	Schreiben	pipeline*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopAutoMLJob	Gewährt die Berechtigung zum Anhalten eines AutoML-Auftrags	Schreiben	automl-job*		
StopCompilationJob	Gewährt die Berechtigung zum Beenden eines Kompilierungsauf	Schreiben	compilation-job*		
StopEdgeDeploymentStage	Erteilt die Berechtigung zum Stoppen einer Edge-Bereitstellungsphase	Schreiben	edge-deployment-plan*		
StopEdgePackagingJob	Gewährt die Berechtigung zum Beenden einer Edge-Verpackungsaufgabe	Schreiben	edge-packaging-job*		
StopHumanLoop	Gewährt die Berechtigung zum Stoppen einer bestimmten menschlichen Schleife	Schreiben	human-loop*		
StopHyperParameterTuningJob	Erteilt die Berechtigung, einen laufenden Hyperparameter-Tuning-Job zu beenden, der über den erstellt wurde CreateHyperParameterTuningJob	Schreiben	hyper-parameter-tuning-job*		
StopInferenceExperiment	Gewährt die Berechtigung zum Beenden eines Inferenzexperiments	Schreiben	inference-experiment*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopInferenceRecommendationsJob	Gewährt die Berechtigung zum Beenden eines Inferenz-Empfehlungsauftrags	Schreiben	inference-recommendations-job*		
StopLabelingJob	Gewährt die Berechtigung zum Stoppen eines Beschriftungsauftrags Alle bereits generierten Kennzeichnungen werden vor dem Beenden exportiert.	Schreiben	labeling-job*		
StopMonitoringSchedule	Gewährt die Berechtigung zum Erstellen eines Überwachungszeitplans.	Schreiben	monitoring-schedule*		
StopNotebookInstance	Gewährt die Berechtigung zum Beenden der Notebook-Instance. Beendet die EC2 Instance. Vor dem Beenden der Instance SageMaker trennt Amazon das EBS-Volume von der Instance. Amazon SageMaker behält das EBS-Volumen bei	Schreiben	notebook-instance*		
StopPipelineExecution	Gewährt die Berechtigung zum Beenden einer Pipeline-Ausführung.	Write	pipeline-execution*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopProcessingJob	Gewährt die Berechtigung zum Beenden eines Verarbeitungsauftrags. Um einen Job zu beenden, SageMaker sendet Amazon dem Algorithmus das SIGTERM-Signal, wodurch die Beendigung des Jobs um 120 Sekunden verzögert wird.	Schreiben	processing-job*		
StopTrainingJob	Gewährt die Berechtigung zum Stoppen einer Trainingsaufgabe Um einen Job zu beenden, SageMaker sendet Amazon dem Algorithmus das SIGTERM-Signal, wodurch die Beendigung des Jobs um 120 Sekunden verzögert wird.	Schreiben	training-job*		
StopTransformJob	Gewährt die Berechtigung zum Stoppen einer Transformationsaufgabe Wenn Amazon eine StopTransformJob Anfrage SageMaker erhält, ändert sich der Status des Jobs in Stopp. Nachdem Amazon den Job SageMaker beendet hat, wird der Status auf Gestoppt gesetzt	Schreiben	transform-job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateAction	Gewährt die Berechtigung zum Aktualisieren einer Aktion.	Schreiben	action*		
UpdateAppImageConfig	Erteilt die Erlaubnis zur Aktualisierung eines AppImageConfig	Schreiben	app-image-config*		
UpdateArtifact	Gewährt die Berechtigung zum Aktualisieren eines Artifacts.	Schreiben	artifact*		
UpdateCluster	Erteilt die Berechtigung zum Aktualisieren eines SageMaker HyperPod Clusters	Schreiben	cluster*		iam:PassRole
UpdateClusterSoftware	Erteilt die Berechtigung zum Aktualisieren der Plattformsoftware für einen SageMaker HyperPod Cluster	Schreiben	cluster*		
UpdateCodeRepository	Erteilt die Erlaubnis zum Aktualisieren eines CodeRepository	Schreiben	code-repository*		
UpdateContext	Gewährt die Berechtigung zum Aktualisieren eines Kontextes.	Write	context*		
UpdateDeviceFleet	Gewährt die Berechtigung zum Aktualisieren einer Geräteflotte	Write	device-fleet*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateDevices	Gewährt die Berechtigung zum Aktualisieren einer Reihe von Geräten	Write	device*		
UpdateDomain	Gewährt die Berechtigung zum Aktualisieren einer Domain	Write	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				sagemaker:VpcSecurityGroupIds sagemaker:InstanceTypes sagemaker:DomainSharingOutputKmsKey sagemaker:ImageArns sagemaker:ImageVersionArns sagemaker:AppNetworkAccessType sagemaker:VpcSubnets	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateEndpoint	Gewährt die Berechtigung zum Aktualisieren eines Endpunkts, damit die in der Anforderung angegebene Endpunktkonfiguration verwendet wird	Write	endpoint*		
			endpoint-config*		
UpdateEndpointWeightsAndCapacities	Gewährt die Berechtigung zum Aktualisieren der Gewichtung und/oder Kapazität einzelner oder mehrerer Varianten, die einem Endpunkt zugeordnet sind	Write	endpoint*		
UpdateExperiment	Gewährt die Berechtigung zum Ausführen eines Experiments	Schreiben	experiment*		
UpdateFeatureGroup	Gewährt die Berechtigung zum Aktualisieren einer Feature-Gruppe	Schreiben	feature-group*		
UpdateFeatureMetadata	Gewährt die Berechtigung zum Aktualisieren der Metadaten eines Features	Schreiben	feature-group*		
UpdateHub	Gewährt die Berechtigung zum Aktualisieren von Hubs	Schreiben	hub*		
UpdateImage	Erteilt die Erlaubnis, die Eigenschaften eines SageMaker Bilds zu aktualisieren	Schreiben	image*		iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateImageVersion	Erteilt die Berechtigung zum Aktualisieren der Eigenschaften eines SageMaker ImageVersion	Schreiben	image-version*		
UpdateInferenceComponent	Gewährt die Berechtigung zum Aktualisieren einer Inferenzkomponente, damit die in der Anforderung angegebenen Spezifikationen und Konfigurationen verwendet werden	Schreiben	inference-component*		
UpdateInferenceComponentRuntimeConfig	Gewährt die Berechtigung zum Aktualisieren der Laufzeitkonfiguration einer angegebenen Inferenzkomponente	Schreiben	inference-component*		
UpdateInferenceExperiment	Gewährt die Berechtigung zum Aktualisieren eines Inferenzexperiments	Schreiben	inference-experiment*		
UpdateModelCard	Gewährt die Berechtigung zum Aktualisieren einer Modellkarte	Schreiben	model-card*		
UpdateModelPackage	Erteilt die Erlaubnis zum Aktualisieren eines ModelPackage	Schreiben	model-package*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				sagemaker:ModelApprovalStatus sagemaker:CustomerMetadataProperties/${MetadataKey} sagemaker:CustomerMetadataPropertiesToRemove	
UpdateMonitoringAlert	Gewährt die Berechtigung zum Aktualisieren einer Überwachungswarnung	Schreiben	monitoring-schedule*		
			monitoring-schedule-alert*		
UpdateMonitoringSchedule	Gewährt die Berechtigung zum Aktualisieren eines Überwachungszeitplans	Write	monitoring-schedule*		iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey sagemaker:VpcSecurityGroupIds	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				sagemaker:VpcSubnets sagemaker:InterContainerTrafficEncryption	
UpdateNotebookInstance	Gewährt die Berechtigung zum Aktualisieren einer Notebook-Instance. Aktualisierungen von Notebook-Instances schließen Upgrades und Downgrades der für die Notebook-Instance verwendeten EC2 Instance zur Anpassung an veränderte Workload-Anforderungen an	Schreiben	notebook-instance*		
				sagemaker:AcceleratorTypes sagemaker:InstanceTypes sagemaker:MinimumInstanceMetadataServiceVersion sagemaker:RootAccess	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateNotebookInstanceLifecycleConfig	Erteilt die Erlaubnis, eine mit der CreateNotebookInstanceLifecycleConfig API erstellte Lebenszykluskonfiguration einer Notebook-Instanz zu aktualisieren	Schreiben	notebook-instance-lifecycle-config*		
UpdatePipeline	Gewährt die Berechtigung zum Aktualisieren einer Pipeline	Write	pipeline*		iam:PassRole
UpdatePipelineExecution	Gewährt die Berechtigung zum Aktualisieren einer Pipeline-Ausführung	Schreiben	pipeline-execution*		
UpdateProject	Gewährt die Berechtigung zum Aktualisieren eines Projekts	Schreiben	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateSharedModel [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren eines freigegebenen Modells	Schreiben	shared-model*		
UpdateSpace	Gewährt die Berechtigung zum Aktualisieren eines Bereichs	Schreiben	space*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				sagemaker:InstanceTypes sagemaker:ImageArns sagemaker:ImageVersionArns sagemaker:OwnerUserProfileArn sagemaker:SpaceSharingType	
UpdateTrainingJob	Gewährt die Berechtigung zum Aktualisieren eines Trainingsauftrags.	Write	training-job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				sagemaker:InstanceTypes sagemaker:KeepAlivePeriod sagemaker:EnableRemoteDebug	
UpdateTrial	Gewährt die Berechtigung zum Aktualisieren eines Tests	Write	experiment-trial*		
UpdateTrialComponent	Gewährt die Berechtigung zum Aktualisieren einer Testkomponente	Schreiben	experiment-trial-component*		
UpdateUserProfile	Erteilt die Erlaubnis zum Aktualisieren eines UserProfile	Schreiben	user-profile*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				sagemaker:InstanceTypes sagemaker:VpcSecurityGroupIds sagemaker:InstanceTypes sagemaker:DomainSharingOutputKmsKey sagemaker:ImageArns sagemaker:ImageVersionArns	
UpdateWorkforce	Gewährt die Berechtigung, eine Belegschaft zu aktualisieren	Write	workforce*		
UpdateWorkteam	Gewährt die Berechtigung, eine Arbeitsgruppe zu aktualisieren	Schreiben	workteam*		

Von Amazon definierte Ressourcentypen SageMaker

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
device	`arn:${Partition}:sagemaker:${Region}:${Account}:device-fleet/${DeviceFleetName}/device/${DeviceName}`	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
device-fleet	`arn:${Partition}:sagemaker:${Region}:${Account}:device-fleet/${DeviceFleetName}`	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
edge-packaging-job	`arn:${Partition}:sagemaker:${Region}:${Account}:edge-packaging-job/${EdgePackagingJobName}`	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
edge-deployment-plan	`arn:${Partition}:sagemaker:${Region}:${Account}:edge-deployment/${EdgeDeploymentPlanName}`	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
human-loop	`arn:${Partition}:sagemaker:${Region}:${Account}:human-loop/${HumanLoopName}`	

Ressourcentypen	ARN	Bedingungsschlüssel
flow-definition	arn:${Partition}:sagemaker:${Region}:${Account}:flow-definition/${FlowDefinitionName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
human-task-ui	arn:${Partition}:sagemaker:${Region}:${Account}:human-task-ui/${HumanTaskUiName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
hub	arn:${Partition}:sagemaker:${Region}:${Account}:hub/${HubName}	
hub-content	arn:${Partition}:sagemaker:${Region}:${Account}:hub-content/${HubName}/${HubContentType}/${HubContentName}	
inference-recommendations-job	arn:${Partition}:sagemaker:${Region}:${Account}:inference-recommendations-job/${InferenceRecommendationsJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
inference-experiment	arn:${Partition}:sagemaker:${Region}:${Account}:inference-experiment/${InferenceExperimentName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
labeling-job	arn:${Partition}:sagemaker:${Region}:${Account}:labeling-job/${LabelingJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
workteam	arn:${Partition}:sagemaker:${Region}:${Account}:workteam/${WorkteamName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
workforce	arn:${Partition}:sagemaker:${Region}:${Account}:workforce/${WorkforceName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
domain	arn:${Partition}:sagemaker:${Region}:${Account}:domain/${DomainId}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
user-profile	arn:${Partition}:sagemaker:${Region}:${Account}:user-profile/${DomainId}/${UserProfileName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
space	arn:${Partition}:sagemaker:${Region}:${Account}:space/${DomainId}/${SpaceName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
app	arn:${Partition}:sagemaker:${Region}:${Account}:app/${DomainId}/${UserProfileName}/${AppType}/${AppName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
app-image-config	arn:${Partition}:sagemaker:${Region}:${Account}:app-image-config/${AppImageConfigName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
studio-lifecycle-config	arn:${Partition}:sagemaker:${Region}:${Account}:studio-lifecycle-config/${StudioLifecycleConfigName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
notebook-instance	arn:${Partition}:sagemaker:${Region}:${Account}:notebook-instance/${NotebookInstanceName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
notebook-instance-lifecycle-config	arn:${Partition}:sagemaker:${Region}:${Account}:notebook-instance-lifecycle-config/${NotebookInstanceLifecycleConfigName}	
code-repository	arn:${Partition}:sagemaker:${Region}:${Account}:code-repository/${CodeRepositoryName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
image	arn:${Partition}:sagemaker:${Region}:${Account}:image/${ImageName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
image-version	`arn:${Partition}:sagemaker:${Region}:${Account}:image-version/${ImageName}/${Version}`	
algorithm	`arn:${Partition}:sagemaker:${Region}:${Account}:algorithm/${AlgorithmName}`	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
cluster	`arn:${Partition}:sagemaker:${Region}:${Account}:cluster/${ClusterId}`	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
training-job	`arn:${Partition}:sagemaker:${Region}:${Account}:training-job/${TrainingJobName}`	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
processing-job	`arn:${Partition}:sagemaker:${Region}:${Account}:processing-job/${ProcessingJobName}`	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
hyper-parameter-tuning-job	`arn:${Partition}:sagemaker:${Region}:${Account}:hyper-parameter-tuning-job/${HyperParameterTuningJobName}`	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Ressource ntypen	ARN	Bedingungsschlüssel
project	arn:${Partition}:sagemaker:${Region}:${Account}:project/${ProjectName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
model-package	arn:${Partition}:sagemaker:${Region}:${Account}:model-package/${ModelPackageName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
model-package-group	arn:${Partition}:sagemaker:${Region}:${Account}:model-package-group/${ModelPackageGroupName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
model	arn:${Partition}:sagemaker:${Region}:${Account}:model/${ModelName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
endpoint-config	arn:${Partition}:sagemaker:${Region}:${Account}:endpoint-config/${EndpointConfigName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
endpoint	arn:${Partition}:sagemaker:${Region}:${Account}:endpoint/${EndpointName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
inference-component	arn:${Partition}:sagemaker:${Region}:${Account}:inference-component/${InferenceComponentName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
transform-job	arn:${Partition}:sagemaker:${Region}:${Account}:transform-job/${TransformJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
compilation-job	arn:${Partition}:sagemaker:${Region}:${Account}:compilation-job/${CompilationJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
automl-job	arn:${Partition}:sagemaker:${Region}:${Account}:automl-job/${AutoMLJobJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
monitoring-schedule	arn:${Partition}:sagemaker:${Region}:${Account}:monitoring-schedule/${MonitoringScheduleName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
monitoring-schedule-alert	arn:${Partition}:sagemaker:${Region}:${Account}:monitoring-schedule/${MonitoringScheduleName}/alert/${MonitoringScheduleAlertName}	

Ressourcentypen	ARN	Bedingungsschlüssel
data-quality-job-definition	arn:${Partition}:sagemaker:${Region}:${Account}:data-quality-job-definition/${DataQualityJobDefinitionName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
model-quality-job-definition	arn:${Partition}:sagemaker:${Region}:${Account}:model-quality-job-definition/${ModelQualityJobDefinitionName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
model-bias-job-definition	arn:${Partition}:sagemaker:${Region}:${Account}:model-bias-job-definition/${ModelBiasJobDefinitionName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
model-explainability-job-definition	arn:${Partition}:sagemaker:${Region}:${Account}:model-explainability-job-definition/${ModelExplainabilityJobDefinitionName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
experiment	arn:${Partition}:sagemaker:${Region}:${Account}:experiment/${ExperimentName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
experiment-trial	arn:${Partition}:sagemaker:${Region}:${Account}:experiment-trial/${TrialName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
experiment-trial-component	arn:${Partition}:sagemaker:${Region}:${Account}:experiment-trial-component/${TrialComponentName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
feature-group	arn:${Partition}:sagemaker:${Region}:${Account}:feature-group/${FeatureGroupName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
pipeline	arn:${Partition}:sagemaker:${Region}:${Account}:pipeline/${PipelineName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
pipeline-execution	arn:${Partition}:sagemaker:${Region}:${Account}:pipeline/${PipelineName}/execution/${RandomString}	
artifact	arn:${Partition}:sagemaker:${Region}:${Account}:artifact/${HashOfArtifactSource}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
context	arn:${Partition}:sagemaker:${Region}:${Account}:context/${ContextName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
action	arn:${Partition}:sagemaker:${Region}:${Account}:action/${ActionName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
lineage-group	arn:${Partition}:sagemaker:${Region}:${Account}:lineage-group/${LineageGroupName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
model-card	arn:${Partition}:sagemaker:${Region}:${Account}:model-card/${ModelCardName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
model-card-export-job	arn:${Partition}:sagemaker:${Region}:${Account}:model-card/${ModelCardName}/export-job/${ExportJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
shared-model	arn:${Partition}:sagemaker:${Region}:${Account}:shared-model/${SharedModelId}	
shared-model-event	arn:${Partition}:sagemaker:${Region}:${Account}:shared-model-event/${EventId}	
sagemaker-catalog	arn:${Partition}:sagemaker:${Region}:${Account}:sagemaker-catalog/${ResourceCatalogName}	

Zustandsschlüssel für Amazon SageMaker

Amazon SageMaker definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach einem Schlüssel, der in der Anfrage des Benutzers an den SageMaker Service enthalten ist	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff anhand eines Tag-Schlüssel-Wert-Paares	String
aws:TagKeys	Filtert Zugriff nach der Liste aller Tag-Schlüsselnamen, die der Ressource in der Anforderung zugeordnet sind	ArrayOfString
sagemaker:AcceleratorTypes	Filtert den Zugriff durch die Liste aller Accelerator-Typen, die der Ressource in der Anforderung zugeordnet sind	ArrayOfString
sagemaker:AppNetworkAccessType	Filtert den Zugriff des App-Netzwerkzugriffstyp, der mit der Ressource in der Anforderung verknüpft ist.	String
sagemaker:CustomerMetadataProperties/${MetadataKey}	Filtert den Zugriff nach einem Metadatenschlüssel-Wert-Paar	String

Bedingungsschlüssel	Beschreibung	Typ
sagemaker:CustomerMetadataPropertiesToRemove	Filtert den Zugriff anhand der Liste der Metadaten eigenschaften, die der Modell-Paket-Ressource in der Anforderung zugeordnet sind	ArrayOfString
sagemaker:DirectInternetAccess	Filtert den Zugriff des direkten Internetzugriffs, der der Ressource in der Anforderung zugeordnet ist.	String
sagemaker:DomainId	Sie können die DomainID als Richtlinienvariable verwenden, um Anfragen von bestimmten SageMaker Domänen zu filtern	String
sagemaker:DomainSharingOutputKmsKey	Filtert den Zugriff durch den KMS-Ausgabeschlüssel der Domain-Freigabe, der der Ressource in der Anforderung zugeordnet ist	ARN
sagemaker:EnableRemoteDebug	Filtert den Zugriff nach der Remote-Debug-Konfiguration in der Anforderung	Bool
sagemaker:FeatureGroupDisableGlueTableCreation	Filtert den Zugriff anhand des DisableGlueTableCreation Flags, das der Featuregruppenressource in der Anfrage zugeordnet ist	Bool
sagemaker:FeatureGroupEnableOnlineStore	Filtert den Zugriff anhand der EnableOnlineStore Markierung, die der Featuregruppe in der Anfrage zugeordnet ist	Bool

Bedingungsschlüssel	Beschreibung	Typ
sagemaker:FeatureGroupOfflineStoreConfig	Filtert den Zugriff nach dem Vorhandensein einer OfflineStoreConfig Ressource aus der Featuregruppe in der Anfrage. Dieser Zugriffsfilter unterstützt nur den Nullbedingungsoperator	Bool
sagemaker:FeatureGroupOfflineStoreKmsKey	Filtert den Zugriff durch den KMS-Schlüssel des Offline-Speichers, der mit der Feature-Gruppenressource in der Anforderung verknüpft ist.	ARN
sagemaker:FeatureGroupOfflineStoreS3Uri	Filtert den Zugriff durch den S3-URI des Offline-Speichers, der mit der Feature-Gruppenressource in der Anforderung verknüpft ist.	Zeichenfolge
sagemaker:FeatureGroupOnlineStoreKmsKey	Filtert den Zugriff durch den KMS-Schlüssel des Online-Speichers, der mit der Feature-Gruppenressource in der Anforderung verknüpft ist.	ARN
sagemaker:FileSystemAccessMode	Filtert den Zugriff durch den Dateisystemzugriffsmodus, der der Ressource in der Anforderung zugeordnet ist.	Zeichenfolge
sagemaker:FileSystemDirectoryPath	Filtert den Zugriff durch den Dateisystem-Verzeichnispfad, der der Ressource in der Anforderung zugeordnet ist.	Zeichenfolge
sagemaker:FileSystemId	Filtert den Zugriff durch eine Dateisystem-ID, die der Ressource in der Anforderung zugeordnet ist.	Zeichenfolge
sagemaker:FileSystemType	Filtert den Zugriff durch eine Dateisystem-ID, die der Ressource in der Anforderung zugeordnet ist.	String

Bedingungsschlüssel	Beschreibung	Typ
sagemaker:HomeEfsFileSystemKmsKey	Filtert den Zugriff nach einem Schlüssel, der in der Anfrage enthalten ist, die der Benutzer an den SageMaker Dienst stellt. Dieser Schlüssel ist veraltet. Es wurde durch Sagemaker ersetzt: VolumeKmsKey	ARN
sagemaker:ImageArns	Filtert den Zugriff nach der Liste aller Image-ARNs, die mit der Ressource in der Anforderung verknüpft sind.	ArrayOfARN
sagemaker:ImageVersionArns	Filtert den Zugriff nach der Liste aller Image-Versions-ARNs, die mit der Ressource in der Anforderung verknüpft sind.	ArrayOfARN
sagemaker:InstanceTypes	Filtert den Zugriff durch die Liste aller Instance-Typen, die der Ressource in der Anforderung zugeordnet sind.	ArrayOfString
sagemaker:InterContainerTrafficEncryption	Filtert den Zugriff durch die Verschlüsselung des Datenverkehrs zwischen Containern, die der Ressource in der Anforderung zugeordnet ist.	Bool
sagemaker:KeepAlivePeriod	Filtert den Zugriff durch den Keep-Alive-Zeitraum, der der Ressource in der Anforderung zugeordnet ist	Numerischer Wert
sagemaker:MaxRuntimeInSeconds	Filtert den Zugriff durch die maximale Laufzeit in Sekunden, die der Ressource in der Anforderung zugeordnet ist.	Numerischer Wert
sagemaker:MinimumInstanceMetadataServiceVersion	Filtert den Zugriff des minimalen Instance-Metadaten-Serviceversion, die von der Ressource in der Anforderung verwendet wird	String
sagemaker:ModelApprovalStatus	Filtert den Zugriff nach dem Genehmigungsstatus des Modells mit dem Modellpaket in der Anforderung	String

Bedingungsschlüssel	Beschreibung	Typ
sagemaker:ModelArn	Filtert den Zugriff durch das Modell, der der Ressource in der Anforderung zugeordnet ist	ARN
sagemaker:NetworkIsolation	Filtert den Zugriff durch die Netzwerkisolation, die der Ressource in der Anforderung zugeordnet ist.	Bool
sagemaker:OutputKmsKey	Filtert den Zugriff durch den KMS-Ausgabeschlüssel, der der Ressource in der Anforderung zugeordnet ist	ARN
sagemaker:OwnerUserProfileArn	Filtert den Zugriff nach dem OwnerUserProfile ARN, der dem Bereich in der Anfrage zugeordnet ist	ARN
sagemaker:ResourceTag/	Filtert den Zugriff nach vorangestellter Zeichenfolge eines Tag-Schlüssel/Wertepaars, das an eine Ressource angefügt ist	Zeichenfolge
sagemaker:ResourceTag/${TagKey}	Filtert den Zugriff anhand eines Tag-Schlüssel-Wert-Paares	Zeichenfolge
sagemaker:RootAccess	Filtert den Zugriff durch den Root-Zugriff, der der Ressource in der Anforderung zugeordnet ist.	String
sagemaker:SearchVisibilityCondition/${FilterKey}	Beschränkt die Ergebnisse Ihrer Suchanfrage auf die Ressourcen, auf die Sie zugreifen können. $ {FilterKey} ist ein Schlüssel, den die VisibilityConditions Konfiguration in der Suchanfrage enthält	String
sagemaker:ServerlessMaxConcurrency	Filtert den Zugriff durch Einschränkung der maximalen Parallelität, die für Serverless-Inferenz in der Anforderung verwendet wird	Numerischer Wert

Bedingungsschlüssel	Beschreibung	Typ
sagemaker:ServerlessMemorySize	Filtert den Zugriff durch Einschränkung der maximalen Arbeitsspeichergröße, die für Serverless-Inferenz in der Anforderung verwendet wird	Numerischer Wert
sagemaker:SpaceSharingType	Filtert den Zugriff durch den Freigabe-Typ, der der Umgebung in der Anforderung zugeordnet ist.	String
sagemaker:TaggingAction	Filtert den Zugriff anhand der API-Aktionen, auf die ein Benutzer Tags anwenden kann. Verwendet den Namen der API-Operation, die eine kennzeichenbare Ressource erstellt, um den Zugriff zu filtern	String
sagemaker:TargetModel	Filtert den Zugriff durch das Zielmodell, das dem Multimodell-Endpunkt in der Anforderung zugeordnet ist.	String
sagemaker:UserProfileName	Sie können die UserProfileName als Richtlinienvariable verwenden, um Anfragen von bestimmten Benutzerprofilen innerhalb einer SageMaker Domain zu filtern. Dieser Kontextschlüssel gilt nicht für Benutzerprofile in gemeinsam genutzten Bereichen	String
sagemaker:VolumeKmsKey	Filtert den Zugriff durch den KMS-Volume-Schlüssel, der der Ressource in der Anforderung zugeordnet ist	ARN
sagemaker:VpcSecurityGroupIds	Filtert den Zugriff über die Liste aller VPC-Sicherheitsgruppen-IDs, die der Ressource in der Anforderung zugeordnet sind	ArrayOfString
sagemaker:VpcSubnets	Filtert den Zugriff über die Liste aller VPC-Subnetze, die der Ressource in der Anforderung zugeordnet sind	ArrayOfString
sagemaker:WorkteamArn	Filtert den Zugriff durch das Arbeitsteam, der der Anforderung zugeordnet ist.	ARN

Bedingungsschlüssel	Beschreibung	Typ
sagemaker:WorkteamType	Filtert den Zugriff des Arbeitsteams, der der Anforderung zugeordnet ist. Dies kann „public-crowd“, „private-crowd“ oder „vendor-crowd“ sein.	String

Aktionen, Ressourcen und Bedingungsschlüssel für Geodatenfunktionen von Amazon SageMaker

Geodatenfunktionen von Amazon SageMaker (Servicepräfix: `sagemaker-geospatial`) stellen die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Aktionen, die von Geodatenfunktionen von Amazon SageMaker definiert wurden
- Von Geodatenfunktionen von Amazon SageMaker definierte Ressourcentypen
- Bedingungsschlüssel für Geodatenfunktionen von Amazon SageMaker

Aktionen, die von Geodatenfunktionen von Amazon SageMaker definiert wurden

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteEarthObservationJob	Gewährt die Berechtigung für den Vorgang DeleteEarthObservationJob, der einen vorhandenen Erdbeobachtungsauftrag löscht	Schreiben	EarthObservationJob*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
DeleteVectorEnrichmentJob	Gewährt die Berechtigung für den Vorgang DeleteVectorEnrichmentJob, der einen vorhandenen Vektoranreicherungsauftrag löscht	Schreiben	VectorEnrichmentJob*		
				aws:ResourceTag/${TagKey}	
ExportEarthObservationJob	Gewährt die Berechtigung zum Kopieren von Ergebnissen eines Erdbeobachtungsauftrags an einen S3-Standort	Schreiben	EarthObservationJob*		iam:PassRole
				aws:ResourceTag/${TagKey}	
ExportVectorEnrichmentJob	Gewährt die Berechtigung zum Kopieren von Ergebnissen eines VectorEnrichmentJob an einen S3-Standort	Schreiben	VectorEnrichmentJob*		iam:PassRole
				aws:ResourceTag/${TagKey}	
GetEarthObservationJob	Gewährt die Berechtigung zum Zurückgeben von Details zum Erdbeobachtungsauftrag	Lesen	EarthObservationJob*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
GetRasterDataCollection	Gewährt die Berechtigung zum Zurückgeben von Details zur Raster-Datensammlung	Lesen	RasterDataCollection*		
				aws:ResourceTag/${TagKey}	
GetTile	Gewährt die Berechtigung zum Erteilen eines Arrays mit einem Auftrag im Bereich Erdbeobachtung	Lesen	EarthObservationJob*		iam:PassRole
GetVectorEnrichmentJob	Gewährt die Berechtigung zum Zurückgeben von Details zum Vektoranreicherungsbereich	Lesen	VectorEnrichmentJob*		
				aws:ResourceTag/${TagKey}	
ListEarthObservationJobs	Gewährt die Berechtigung zum Zurückgeben einer Reihe von Erdbeobachtungsaufträgen, die dem aktuellen Konto zugeordnet sind	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListRasterDataCollections	Gewährt die Berechtigung zum Zurückgeben eines Arrays der Aster-Datensammlungen, die dem angegebenen Modellnamen zugeordnet sind	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten einer Geodatenressource von SageMaker	Auflisten	EarthObservationJob		
			RasterDataCollection		
			VectorEnrichmentJob		
				aws:ResourceTag/${TagKey}	
ListVectorEnrichmentJobs	Gewährt die Berechtigung zum Zurückgeben eines Arrays von Vektoranreicherungsaufträgen, die dem aktuellen Konto und Endpunkt zugeordnet sind	Auflisten			
SearchRasterDataCollection	Gewährt die Berechtigung zum Abfragen von Raster-Datensammlungen	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartEarthObservationJob	Gewährt die Berechtigung für den Vorgang StartEarthObservationJob, der einen neuen Erdbeobachtungsauftrag für Ihr Konto startet	Schreiben	EarthObservationJob*		iam:PassRole sagemaker-geospatial:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
StartVectorEnrichmentJob	Gewährt die Berechtigung für den Vorgang StartVectorEnrichmentJob, der einen neuen Vektoranreicherungsauftrag für Ihr Konto startet	Schreiben	VectorEnrichmentJob*		iam:PassRole sagemaker-geospatial:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopEarthObservationJob	Gewährt die Berechtigung für den Vorgang StopEarthObservationJob, der einen bestehenden Erdbeobachtungsauftrag beendet	Schreiben	EarthObservationJob*		
				aws:ResourceTag/${TagKey}	
StopVectorEnrichmentJob	Gewährt die Berechtigung für den Vorgang StopVectorEnrichmentJob, der einen vorhandenen Vektoranreicherungsauftrag beendet	Schreiben	VectorEnrichmentJob*		
				aws:ResourceTag/${TagKey}	
TagResource	Gewährt die Berechtigung zum Markieren einer Geodatenressource von SageMaker	Markierung	EarthObservationJob		
			RasterDataCollection		
			VectorEnrichmentJob		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Geodatenressource von SageMaker	Markierung	EarthObservationJob		
			RasterDataCollection		
			VectorEnrichmentJob		
				aws:TagKeys	

Von Geodatenfunktionen von Amazon SageMaker definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
EarthObservationJob	`arn:${Partition}:sagemaker-geospatial:${Region}:${Account}:earth-observation-job/${JobID}`	aws:ResourceTag/${TagKey}
RasterDataCollection	`arn:${Partition}:sagemaker-geospatial:${Region}:${Account}:raster-data-collection/${CollectionID}`	aws:ResourceTag/${TagKey}
VectorEnrichmentJob	`arn:${Partition}:sagemaker-geospatial:${Region}:${Account}:vector-enrichment-job/${JobID}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Geodatenfunktionen von Amazon SageMaker

Geodatenfunktionen von Amazon SageMaker definieren die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon SageMaker Ground Truth Synthetic

Amazon SageMaker Ground Truth Synthetic (Servicepräfix: `sagemaker-groundtruth-synthetic`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon SageMaker Ground Truth Synthetic definierte Aktionen
- Von Amazon SageMaker Ground Truth Synthetic definierte Ressourcentypen
- Bedingungsschlüssel für Amazon SageMaker Ground Truth Synthetic

Von Amazon SageMaker Ground Truth Synthetic definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateProject [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines Projekts	Schreiben			
DeleteProject [nur Berechtigung]	Gewährt die Berechtigung zum Löschen eines Projekts	Write			
GetAccountDetails [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Kontodetails	Lesen			
GetBatch [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen eines Batches	Lesen			
GetProject [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen eines Projekts	Lesen			
ListBatchDataTransfers [nur Berechtigung]	Erteilt die Berechtigung zum Auflisten von Batch-Datenübertragungen	Auflisten			
ListBatchSummaries [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Batch-Zusammenfassungen	Auflisten			
ListProjectDataTra	Erteilt die Berechtigung zum Auflisten von Projektdatenübertragungen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
nsfers [nur Berechtigung]					
ListProjectSummaries [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Projekten-Zusammenfassungen	Auflisten			
StartBatchDataTransfer [nur Berechtigung]	Erteilt die Berechtigung zum Starten einer Batch-Datenübertragung	Schreiben			
StartProjectDataTransfer [nur Berechtigung]	Erteilt die Berechtigung zum Starten einer Projektdatenübertragung	Schreiben			
UpdateBatch [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren eines Batches	Schreiben			

Von Amazon SageMaker Ground Truth Synthetic definierte Ressourcentypen

Amazon SageMaker Ground Truth Synthetic unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf Amazon SageMaker Ground Truth Synthetic zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für Amazon SageMaker Ground Truth Synthetic

SageMaker Ground Truth Synthetic hat keine service-spezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienaussagen verwendet werden können. Eine Liste der globalen

Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Savings Plans

AWS Savings Plans (Dienstpräfix:`savingsplans`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Savings Plans definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie

den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSavingsPlan	Gewährt die Berechtigung zum Erstellen eines Savings Plan	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteQueuedSavingsPlan	Gewährt die Berechtigung zum Löschen des mit dem Kundenkonto verknüpften Savings Plan in der Warteschlange	Write	savingsplan*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
DescribeSavingsPlanRates	Gewährt die Berechtigung zur Beschreibung der mit dem Savings Plan des Kunden verbundenen Tarife	Read	savingsplan*		
				aws:ResourceTag/${TagKey}	
DescribeSavingsPlans	Gewährt die Berechtigung zur Beschreibung der mit dem Kundenkonto verbundenen Savings Plans	Read	savingsplan*		
				aws:ResourceTag/${TagKey}	
DescribeSavingsPlansOfferingRates	Gewährt die Berechtigung zur Beschreibung der mit den Savings Plans-Angeboten verbundenen Tarife	Read			
DescribeSavingsPlansOfferings	Gewährt die Berechtigung zur Beschreibung der Savings Plans-Angebote, die der Kunde erwerben kann	Read			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für einen Savings Plan	Auflisten	savingsplan*		
ReturnSavingsPlan	Erteilt die Erlaubnis, einen Sparplan zurückzugeben	Schreiben	savingsplan*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
TagResource	Gewährt die Berechtigung zum Markieren eines Savings Plan	Markieren	savingsplan*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung eines Savings Plan	Markieren	savingsplan*		
				aws:TagKeys	

Von AWS Savings Plans definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
savingsplan	`arn:${Partition}:savingsplans::${Account}:savingsplan/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Savings Plans

AWS Savings Plans definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den zulässigen Werten für jeden der Tags	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Tag-Wert, der der Ressource zugeordnet ist	String
aws:TagKeys	Filtert den Zugriff nach dem Vorhandensein verbindlicher Tags in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Secrets Manager

AWS Secrets Manager (Dienstpräfix:`secretsmanager`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Secrets Manager definierte Aktionen
- Von AWS Secrets Manager definierte Ressourcentypen
- Bedingungsschlüssel für AWS Secrets Manager

Von AWS Secrets Manager definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetSecretValue	Gewährt die Berechtigung zum Abrufen und Entschlüsseln einer Liste von Geheimnissen	Auflisten			
CancelRotateSecret	Gewährt die Berechtigung zum Abbrechen einer laufenden Geheimnisdrehung	Schreiben	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSecret	Gewährt die Berechtigung zum Erstellen eines Geheimnisses, das verschlüsselte Daten speichert, die abgefragt und gedreht werden können	Schreiben	Secret*	secretsmanager:Name secretsmanager:Description secretsmanager:KmsKeyId aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys secretsmanager:ResourceTag/tag-key secretsmanager:AddReplicaRegions	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				secretsmanager:ForceOverwriteReplicaSecret	
DeleteResourcePolicy	Gewährt die Berechtigung zum Löschen der Ressourcenrichtlinie, die an ein Geheimnis angefügt ist	Berechtigungsverwaltung	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteSecret	Gewährt die Berechtigung zum Löschen eines Geheimnisses	Schreiben	Secret*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:RecoveryWindowInDays secretsmanager:ForceDeleteWithoutRecovery secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:Sec	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				retPrimaryRegion	
DescribeSecret	Gewährt die Berechtigung zum Abrufen der Metadaten über ein Geheimnis, aber nicht die verschlüsselten Daten	Lesen	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
GetRandomPassword	Gewährt die Berechtigung zum Generieren einer zufälligen Zeichenfolge zur Verwendung bei der Passworterstellung	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetResourcePolicy	Gewährt die Berechtigung zum Abrufen der Ressourcenrichtlinie, die an ein Geheimnis angefügt ist	Lesen	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
GetSecretValue	Gewährt die Berechtigung zum Abrufen und Entschlüsseln der verschlüsselten Daten	Lesen	Secret*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				secretsmanager:SecretId secretsmanager:VersionId secretsmanager:VersionStage secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListSecretVersionIds	Gewährt die Berechtigung zum Auflisten der verfügbaren Versionen eines Geheimnisses	Lesen	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
ListSecrets	Gewährt die Berechtigung zum Auflisten der verfügbaren Geheimnisse	Auflisten			
PutResourcePolicy	Gewährt die Berechtigung zum Anfügen einer Ressourcenrichtlinie an ein Geheimnis	Berechtigungsverwaltung	Secret*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:BlockPublicPolicy secretsmanager:SecretPrimaryRegion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutSecretValue	Gewährt die Berechtigung zum Erstellen einer neuen Version des Geheimnisses mit neuen verschlüsselten Daten	Schreiben	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
RemoveRegionsFromReplication	Gewährt die Berechtigung zum Entfernen von Regionen aus der Replikation	Schreiben	Secret*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ReplicateSecretToRegions	Gewährt die Berechtigung zum Konvertieren eines bestehenden Geheimnisses in ein Multi-Region-Geheimnis und zum Starten der Replikation des Geheimnisses in eine Liste neuer Regionen	Schreiben	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:AddReplicaRegions secretsmanager:For	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ceOverwriteReplicaSecret	
RestoreSecret	Gewährt die Berechtigung zum Abbrechen des Löschens eines Geheimnisses	Schreiben	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
RotateSecret	Gewährt die Berechtigung zum Starten der Drehung eines Geheimnisses	Schreiben	Secret*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				secretsmanager:SecretId secretsmanager:RotationLambdaARN secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:Mod	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ifyRotationRules secretsmanager:RotateImmediately	
StopReplicationToReplica	Gewährt die Berechtigung zum Entfernen des Geheimnisses aus der Replikation und zum Konvertieren des Geheimnisses in ein regionales Geheimnis in der Replikatregion	Schreiben	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einem Geheimnis	Tagging	Secret*	secretsmanager:SecretId aws:RequestTag/${TagKey} aws:TagKeys secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einem Geheimnis	Tagging	Secret*	secretsmanager:SecretId aws:TagKeys secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateSecret	Gewährt die Berechtigung zum Aktualisieren eines Geheimnisses mit neuen Metadaten oder mit einer neuen Version der verschlüsselten Daten	Schreiben	Secret*	secretsmanager:SecretId secretsmanager:Description secretsmanager:KmsKeyId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:Sec	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				retPrimaryRegion	
UpdateSecretVersionStage	Gewährt die Berechtigung, eine Stufe von einem Geheimnis zum anderen zu verschieben	Schreiben	Secret*		
				secretsmanager:SecretId secretsmanager:VersionStage secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ValidateResourcePolicy	Gewährt die Berechtigung zum Validieren einer Ressourcenrichtlinie vor dem Anhängen einer Richtlinie	Berechtigungsverwaltung	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Von AWS Secrets Manager definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Secret	`arn:${Partition}:secretsmanager:${Region}:${Account}:secret:${SecretId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys secretsmanager:ResourceTag/tag-key secretsmanager:resource/AllowRotationLambdaArn

Bedingungsschlüssel für AWS Secrets Manager

AWS Secrets Manager definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach einem Schlüssel, der in der Anforderung vorhanden ist, die der Benutzer an den Secrets-Manager-Service sendet	String

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	String
aws:TagKeys	Filtert den Zugriff nach der Liste aller Tag-Schlüsselnamen, die in der Anforderung vorhanden sind, die der Benutzer an den Secrets-Manager-Service sendet	ArrayOfString
secretsmanager:AddReplicaRegions	Filtert den Zugriff nach der Liste der Regionen, in denen das Geheimnis repliziert werden soll	ArrayOfString
secretsmanager:BlockPublicPolicy	Filtert den Zugriff danach, ob die Ressourcenrichtlinie den breiten AWS-Konto Zugriff blockiert	Bool
secretsmanager:Description	Filtert den Zugriff nach dem Beschreibungstext in der Anforderung	String
secretsmanager:ForceDeleteWithoutRecovery	Filtert den Zugriff basierend darauf, ob das Geheimnis sofort und ohne Wiederherstellungsfenster gelöscht werden soll	Bool
secretsmanager:ForceOverwriteReplicaSecret	Filtert den Zugriff danach, ob ein Secret mit demselben Namen in der Zielregion überschrieben werden soll	Bool
secretsmanager:KmsKeyId	Filtert den Zugriff anhand der Schlüssel-ID des KMS-Schlüssels in der Anfrage	String
secretsmanager:ModifyRotationRules	Filtert den Zugriff danach, ob die Rotationsregeln des Secrets geändert werden sollen	Bool

Bedingungsschlüssel	Beschreibung	Typ
secretsmanager:Name	Filtert den Zugriff nach dem Anzeigenamen des Geheimnisses in der Anforderung	String
secretsmanager:RecoveryWindowInDays	Filtert den Zugriff anhand der Anzahl der Tage, die Secrets Manager wartet, bevor das Geheimnis gelöscht werden kann	Numerischer Wert
secretsmanager:ResourceTag/tag-key	Filtert den Zugriff anhand eines Tag-Schlüssel-Wert-Paares	String
secretsmanager:RotateImmediately	Filtert den Zugriff danach, ob das Secret sofort rotiert werden soll	Bool
secretsmanager:RotationLambdaARN	Filtert den Zugriff durch den ARN der Lambda-Funktion für die Drehung in der Anforderung	ARN
secretsmanager:SecretId	Filtert den Zugriff durch den SecretID-Wert in der Anforderung	ARN
secretsmanager:SecretPrimaryRegion	Filtert den Zugriff nach der primären Region, in der das Geheimnis erstellt wird	String
secretsmanager:VersionId	Filtert den Zugriff nach der eindeutigen Kennung der Geheimnisversion in der Anforderung	String
secretsmanager:VersionStage	Filtert den Zugriff nach der Liste von Versionsstufen in der Anforderung	String

Bedingungsschlüssel	Beschreibung	Typ
secretsmanager:resource/AllowRotationLambdaArn	Filtert den Zugriff nach dem ARN der Lambda-Funktion für die Drehung, die dem Geheimnis zugeordnet ist	ARN

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Security Hub

AWS Security Hub (Servicepräfix: `securityhub`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Security Hub definierte Aktionen
- Von AWS Security Hub definierte Ressourcentypen
- Bedingungsschlüssel für AWS Security Hub

Von AWS Security Hub definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptAdministratorInvitation	Gewährt die Berechtigung zum Akzeptieren von Security Hub-Einladungen, ein Mitgliedskonto zu werden	Write	hub		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptInvitation	Gewährt die Berechtigung zum Akzeptieren von Security Hub-Einladungen, ein Mitgliedskonto zu werden	Schreiben	hub		
BatchDeleteAutomationRules	Gewährt die Berechtigung zum Löschen einer oder mehrerer Automatisierungsregeln in Security Hub	Schreiben	automation-rule*		
BatchDisableStandards	Gewährt die Berechtigung zum Deaktivieren von Standards in Security Hub	Write	hub		
BatchEnableStandards	Gewährt die Berechtigung zum Aktivieren von Standards in Security Hub	Schreiben	hub		
BatchGetAutomationRules	Gewährt die Berechtigung zum Abrufen einer Liste von Details für Automatisierungsregeln von Security Hub auf der Amazon-Ressourcennamen (ARNs)-Regel	Lesen	automation-rule*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetConfigurationPolicyAssociations	Gewährt die Berechtigung zum Abrufen von Informationen über Konfigurationsrichtlinien, die mit einer bestimmten Liste von Mitgliedskonten und Organisationseinheiten der Organisation des aufrufenden Kontos verknüpft sind	Lesen			
BatchGetControlEvaluations [nur Berechtigung]	Gewährt die Berechtigung, den Enablement- und Compliance-Status von Kontrollen, die Anzahl der Befunde für Kontrollen und die Gesamtsicherheitsbewertung für Kontrollen in der Security-Hub-Konsole abzurufen	Lesen	hub		
BatchGetSecurityControls	Gewährt die Berechtigung zum Abrufen von Details zu bestimmten Sicherheitskontrollen, die per ID oder ARN identifiziert werden	Lesen			securityhub:DescribeStandardsControls
BatchGetStandardsControlAssociations	Gewährt die Berechtigung zum Abrufen des Aktivierungsstatus einer Reihe von Sicherheitskontrollen in Standards	Lesen			securityhub:DescribeStandardsControls

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchImportFindings	Gewährt die Berechtigung zum Importieren von Ergebnissen in Security Hub von einem integrierten Produkt	Schreiben	product*		
				securityhub:TargetAccount	
BatchUpdateAutomationRules	Gewährt die Berechtigung, eine oder mehrere Automatisierungsregeln vom Security Hub aus zu aktualisieren, basierend auf der Amazon-Ressourcennamen (ARNs)-Regel und Eingabeparametern	Schreiben	automation-rule*		
BatchUpdateFindings	Gewährt die Berechtigung zum Aktualisieren von kundengesteuerten Feldern für einen ausgewählten Satz von Security Hub-Ergebnissen	Schreiben	hub		
				securityhub:ASFFSyntaxPath/${ASFFSyntaxPath}	
BatchUpdateStandardsControlAssociations	Gewährt die Berechtigung zum Aktualisieren des Aktivierungsstatus einer Reihe von Sicherheitskontrollen in Standards	Schreiben			securityhub:UpdateStandardsControl
CreateActionTarget	Gewährt die Berechtigung zum Erstellen benutzerdefinierter Aktionen in Security Hub	Schreiben	hub		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAutomationRule	Gewährt die Berechtigung zum Erstellen einer Automatisierungsregel basierend auf Eingabeparametern	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfigurationPolicy	Gewährt die Berechtigung zum Erstellen einer Konfigurationsrichtlinie zur Verwaltung der Einstellungen von Organisationsmitgliedern in Security Hub	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFindingAggregator	Gewährt die Berechtigung zum Erstellen eines Ergebnis-Aggregators, der die Konfiguration für die regionsübergreifende Ergebnis-Aggregation enthält	Schreiben			
CreateInsight	Gewährt die Berechtigung zum Erstellen von Insights in Security Hub. Insights sind Sammlungen verwandter Ergebnisse	Write	hub		
CreateMembers	Gewährt die Berechtigung zum Erstellen von Mitgliedskonten in Security Hub	Write	hub		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeclineInvitations	Gewährt die Berechtigung zum Ablehnen von Security Hub-Einladungen, ein Mitgliedskonto zu werden	Write	hub		
DeleteActionTarget	Gewährt die Berechtigung zum Löschen benutzerdefinierter Aktionen in Security Hub	Schreiben	hub		
DeleteConfigurationPolicy	Gewährt die Berechtigung zum Löschen eines vorhandenen Konfigurationssatzes	Schreiben	configuration-policy*		
DeleteFindingAggregator	Gewährt die Berechtigung zum Löschen eines Ergebnis-Aggregators, der die Ergebnis-Aggregation über Regionen hinweg deaktiviert	Schreiben	finding-aggregator*		
DeleteInsight	Gewährt die Berechtigung zum Löschen von Insights aus Security Hub	Write	hub		
DeleteInvitations	Gewährt die Berechtigung zum Löschen von Security Hub-Einladungen, ein Mitgliedskonto zu werden	Write	hub		
DeleteMembers	Gewährt die Berechtigung zum Löschen von Security Hub-Mitgliedskonten	Write	hub		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeActionTargets	Gewährt die Berechtigung zum Abrufen einer Liste der benutzerdefinierten Aktionen mithilfe der API	Read	hub		
DescribeHub	Gewährt die Berechtigung zum Abrufen von Informationen über die Hub-Ressource in Ihrem Konto	Read	hub		
DescribeOrganizationConfiguration	Gewährt die Berechtigung zum Beschreiben der Organisationskonfiguration für Security Hub	Read	hub		
DescribeProducts	Gewährt die Berechtigung zum Abrufen von Informationen über die verfügbaren Security Hub-Produktintegrationen	Read	hub		
DescribeStandards	Gewährt die Berechtigung zum Abrufen von Informationen zu Security Hub-Standards	Read	hub		
DescribeStandardsControls	Gewährt die Berechtigung zum Abrufen von Informationen zu Security Hub-Standardkontrollen	Read	hub		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisableImportFindingsForProduct	Gewährt die Berechtigung zum Deaktivieren des Ergebnisimports für ein in Security Hub integriertes Produkt	Write	hub		
DisableOrganizationAdminAccount	Gewährt die Berechtigung zum Entfernen des Security Hub-Administratorkontos für Ihre Organisation	Write	hub		organizations:DescribeOrganization
DisableSecurityHub	Gewährt die Berechtigung zum Deaktivieren von Security Hub	Write	hub		
DisassociateFromAdministratorAccount	Gewährt die Berechtigung für ein Security-Hub-Mitgliedskonto, die Verknüpfung mit dem zugehörigen Administratorkonto aufzuheben	Write	hub		
DisassociateFromMasterAccount	Gewährt die Berechtigung für ein Security Hub-Mitgliedskonto, die Verknüpfung mit dem zugehörigen Masterkonto aufzuheben	Write	hub		
DisassociateMembers	Gewährt die Berechtigung zum Aufheben der Verknüpfung von Security-Hub-Mitgliedskonten mit dem zugehörigen Administratorkonto	Write	hub		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
EnableImportFindingsForProduct	Gewährt die Berechtigung zum Aktivieren des Ergebnisimports für ein in Security Hub integriertes Produkt	Write	hub		
EnableOrganizationAdminAccount	Gewährt die Berechtigung zum Bestimmen eines Security Hub-Administratorkontos für Ihre Organisation	Write	hub		organizations:DescribeOrganization organizations:EnableAWSServiceAccess organizations:RegisterDelegatedAdministrator
EnableSecurityHub	Gewährt die Berechtigung zum Aktivieren von Security Hub	Write	hub	aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAdhocInsightResults [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Erkenntnissergebnissen durch Bereitstellen einer Reihe von Filtern anstelle eines Einblick-ARN	Read	hub		
GetAdministratorAccount	Gewährt die Berechtigung zum Abrufen von Details zum Security-Hub-Administratorkonto	Lesen	hub		
GetConfigurationPolicy	Gewährt die Berechtigung, sich einen vollständigen Überblick über eine Konfigurationsrichtlinie zu verschaffen, die vom aufrufenden Konto erstellt wurde	Lesen	configuration-policy*		
GetConfigurationPolicyAssociation	Gewährt die Berechtigung zum Abrufen von Informationen über eine Konfigurationsrichtlinie, die einem Mitgliedskonto oder einer Organisationseinheit der Organisation des anrufenden Accounts zugeordnet ist	Lesen			
GetControlFindingSummary [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen einer Sicherheitsbewertung sowie der Anzahl der Such- und Kontrollstatus für einen Sicherheitsstandard	Read	hub		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetEnabledStandards	Gewährt die Berechtigung zum Abrufen einer Liste von Standards, die in Security Hub aktiviert sind	Auflisten	hub		
GetFindingAggregator	Gewährt die Berechtigung zum Abrufen von Details für einen Ergebnis-Aggregator, der die Ergebnis-Aggregation über Regionen hinweg konfiguriert	Lesen	finding-aggregator *		
GetFindingHistory	Gewährt die Berechtigung zum Abrufen einer Liste mit vergangenen Erkenntnissen vom Security Hub	Lesen	hub		
GetFindings	Gewährt die Berechtigung zum Abrufen einer Liste von Ergebnissen von Security Hub	Read	hub		
GetFreeTrialEndDate [nur Berechtigung]	Gewährt die Berechtigung, das Enddatum für die kostenlose Testversion eines Kontos von Security Hub abzurufen	Read	hub		
GetFreeTrialUsage [nur Berechtigung]	Gewährt die Berechtigung, Informationen über die Nutzung von Security Hub während der kostenlosen Testphase abzurufen	Read	hub		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetInsightFindingTrend [nur Berechtigung]	Gewährt die Berechtigung, einen Erkenntnisfindetrend von Security Hub abzurufen, um ein Diagramm zu generieren	Read	hub		
GetInsightResults	Gewährt die Berechtigung zum Abrufen von Insight-Ergebnissen von Security Hub	Read	hub		
GetInsights	Gewährt die Berechtigung zum Abrufen von Security Hub-Insights	List	hub		
GetInvitationsCount	Gewährt die Berechtigung zum Abrufen der Anzahl der Security Hub-Mitgliedschaftseinladungen, die an das Konto gesendet wurden	Read	hub		
GetMasterAccount	Gewährt die Berechtigung zum Abrufen von Details zum Security Hub-Masterkonto	Read	hub		
GetMembers	Gewährt die Berechtigung zum Abrufen der Details von Security Hub-Mitgliedskonten	Lesen	hub		
GetSecurityControlDefinition	Gewährt die Berechtigung, die Definitionsdetails einer bestimmten, durch die ID identifizierten Sicherheitskontrolle abzurufen	Lesen			securityhub:DescribeStandardsControls

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetUsage [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Informationen zu Security Hub-Standards	Read	hub		
InviteMembers	Gewährt die Berechtigung zum Einladen anderer AWS-Konten, Security-Hub-Mitgliedskonten zu werden	Schreiben	hub		
ListAutomationRules	Gewährt die Berechtigung zum Abrufen einer Liste von Automatisierungsregeln und deren Metadaten für das anrufende Konto von Security Hub	Auflisten			
ListConfigurationPolicies	Gewährt die Berechtigung zum Auflisten von Zusammenfassungen aller vom aufrufenden Konto erstellten Konfigurationsrichtlinien	Auflisten			
ListConfigurationPolicyAssociations	Gewährt die Berechtigung zum Abrufen von Informationen über alle Konfigurationsrichtlinien, die allen Mitgliedskonten und Organisationseinheiten der Organisation des anrufenden Accounts zugeordnet sind	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListControlEvaluationSummaries [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen einer Liste von Steuerelementen für einen Standard, einschließlich der Steuerelement-IDs, Status und Ergebniszählungen	Read	hub		
ListEnabledProductsForImport	Gewährt die Berechtigung zum Abrufen der in Security Hub integrierten Produkte, die derzeit aktiviert sind	Auflisten	hub		
ListFindingAggregators	Gewährt die Berechtigung zum Abrufen einer Liste von Ergebnis-Aggregatoren, die die Konfiguration für die regionsübergreifende Ergebnis-Aggregation enthält	Auflisten			
ListInvitations	Gewährt die Berechtigung zum Abrufen der Security Hub-Einladungen, die an das Konto gesendet wurden	List	hub		
ListMembers	Gewährt die Berechtigung zum Abrufen von Details zu Security-Hub-Mitgliedskonten, die mit dem Administratorkonto verknüpft sind	List	hub		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListOrganizationAdminAccounts	Gewährt die Berechtigung zum Auflisten der Security Hub-Administratorkonten für Ihre Organisation	Auflisten	hub		organizations:DescribeOrganization
ListSecurityControlDefinitions	Gewährt die Berechtigung zum Abrufen einer Liste von Sicherheitskontrolldefinitionen, die Details zu Sicherheitskontrollen in der aktuellen Region enthalten	Auflisten			
ListStandardsControlAssociations	Gewährt die Berechtigung zum Auflisten des Aktivierungsstatus einer Sicherheitskontrolle in Standards	Auflisten			securityhub:DescribeStandardsControls
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags, die mit einer Ressource verknüpft sind	Read	automation-rule		
			configuration-policy		
			hub		
SendFindingEvents [nur Berechtigung]	Gewährt die Berechtigung zum Verwenden einer benutzerdefinierten Aktion zum Senden von Security Hub-Ergebnissen an Amazon EventBridge	Lesen	hub		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SendInsightEvents [nur Berechtigung]	Gewährt die Berechtigung zum Verwenden einer benutzerdefinierten Aktion zum Senden von Security Hub-Insights an Amazon EventBridge	Lesen	hub		
StartConfigurationPolicyAssociation	Gewährt die Berechtigung, eine Konfigurationsrichtlinie einem Mitgliedskonto oder einer Organisationseinheit in der Organisation des anrufenden Accounts zuzuordnen	Schreiben	configuration-policy		
StartConfigurationPolicyDisassociation	Gewährt die Berechtigung, eine Konfigurationsrichtlinienverknüpfung von einem Mitgliedskonto oder einer Organisationseinheit in der Organisation des anrufenden Kontos zu entfernen	Schreiben	configuration-policy		
TagResource	Gewährt die Berechtigung, Tags zu einer Security Hub-Ressource hinzuzufügen	Markieren	automation-rule		
			configuration-policy		
			hub		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags von einer Security Hub-Ressource	Markieren	automation-rule		
			configuration-policy		
			hub		
UpdateActionTarget	Gewährt die Berechtigung zum Aktualisieren benutzerdefinierter Aktionen in Security Hub	Schreiben	hub		
UpdateConfigurationPolicy	Gewährt die Berechtigung zum Aktualisieren einer bestehenden Lizenzkonfiguration	Schreiben	configuration-policy*		
UpdateFindingAggregator	Gewährt die Berechtigung zum Aktualisieren eines Ergebnis-Aggregators, der die Konfiguration für die regionsübergreifende Ergebnis-Aggregation enthält	Schreiben	finding-aggregator*		
UpdateFindings	Gewährt die Berechtigung zum Aktualisieren von Security Hub-Ergebnissen	Write	hub		
UpdateInsight	Gewährt die Berechtigung zum Aktualisieren von Insights in Security Hub	Write	hub		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateOrganizationConfiguration	Gewährt die Berechtigung zum Aktualisieren der Organisationskonfiguration für Security Hub	Schreiben	hub		
UpdateSecurityControl	Gewährt die Berechtigung zum Aktualisieren von Eigenschaften einer bestimmten Sicherheitskontrolle, die durch ID oder ARN identifiziert wird	Schreiben			securityhub:UpdateStandardsControl
UpdateSecurityHubConfiguration	Gewährt die Berechtigung zur Aktualisierung der Security Hub-Konfiguration	Write	hub		
UpdateStandardsControl	Gewährt die Berechtigung zum Aktualisieren der Security Hub-Standardkontrollen	Write	hub		

Von AWS Security Hub definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
hub	`arn:${Partition}:securityhub:${Region}:${Account}:hub/default`	aws:ResourceTag/${TagKey}
product	`arn:${Partition}:securityhub:${Region}:${Account}:product/${Company}/${ProductId}`	
finding-aggregator	`arn:${Partition}:securityhub:${Region}:${Account}:finding-aggregator/${FindingAggregatorId}`	
automation-rule	`arn:${Partition}:securityhub:${Region}:${Account}:automation-rule/${AutomationRuleId}`	
configuration-policy	`arn:${Partition}:securityhub:${Region}:${Account}:configuration-policy/${ConfigurationPolicyId}`	

Bedingungsschlüssel für AWS Security Hub

AWS Security Hub definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff danach, ob Tag-Schlüssel-Wert-Paare in der Anforderung vorhanden sind	String

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tag-Schlüssel-Wert-Paaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert Zugriff basierend auf dem Vorhandensein von Tag-Schlüsseln in der Anforderung	ArrayOfString
securityhub:ASFFSyntaxPath/${ASFFSyntaxPath}	Filtert den Zugriff nach den angegebenen Feldern und Werte in der Anforderung	String
securityhub:TargetAccount	Filtert den Zugriff nach dem AwsAccountId Feld, das in der Anforderung angegeben ist	String

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Security Lake

Amazon Security Lake (Servicepräfix: `securitylake`) stellt die folgenden Servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Security Lake definierte Aktionen
- Von Amazon Security Lake definierte Ressourcentypen

- Bedingungsschlüssel für Amazon Security Lake

Von Amazon Security Lake definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWSzu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAwsLogSource	Gewährt die Berechtigung zum Aktivieren jedes Quelltyps in einer beliebigen Region für Konten, die entweder Teil einer vertrauenswürdigen Organisation oder eigenständige Konten sind	Schreiben	data-lake *		glue:CreateDatabase glue:CreateTable glue:GetDatabase glue:GetTable iam:CreateServiceLinkedRole kms:CreateGrant kms:DescribeKey
CreateCustomLogSource	Gewährt die Berechtigung zum Hinzufügen einer benutzerdefinierten Quelle	Schreiben	data-lake *		glue:CreateCrawler glue:CreateDatabase glue:CreateTable

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					glue:StartCrawlerSchedule iam:DeleteRolePolicy iam:GetRole iam:PassRole iam:PutRolePolicy kms:CreateGrant kms:DescribeKey kms:GenerateDataKey lakeformation:GrantPermissions lakeformation:Regi

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					sterResource s3:ListBucket s3:PutObject

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDataLake	Gewährt die Berechtigung zum Erstellen eines neuen Security Data Lake	Schreiben	data-lake *		events:PutRule events:PutTargets iam:CreateServiceLinkedRole iam:DeleteRolePolicy iam:GetRole iam:ListAttachedRolePolicies iam:PassRole iam:PutRolePolicy kms:CreateGrant kms:DescribeKey lakeformation:GetD

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ataLakeSettings lakeformation:PutDataLakeSettings lambda:AddPermission lambda:CreateEventSourceMapping lambda:CreateFunction organizations:DescribeOrganization organizations:ListAccounts organizations:ListDelegatedServicesF

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					orAccount s3:CreateBucket s3:GetObject s3:GetObjectVersion s3:ListBucket s3:PutBucketPolicy s3:PutBucketPublicAccessBlock s3:PutBucketVersioning sqs:CreateQueue sqs:GetQueueAttributes

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					sqs:SetQueueAttributes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataLakeExceptionSubscription	Gewährt die Berechtigung zum Erhalten von sofortigen Benachrichtigungen über Ausnahmen. Abonniert SNS-Themen für Ausnahmebenachrichtigungen	Schreiben			
CreateDataLakeOrganizationConfiguration	Gewährt die Berechtigung, Amazon Security Lake automatisch für neue Mitgliedskonten in Ihrer Organisation zu aktivieren	Schreiben	data-lake*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSubscriber	Gewährt die Berechtigung zum Erstellen eines Subscribers	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateRole iam:DeleteRolePolicy iam:GetRole iam:PutRolePolicy lakeformation:GrantPermissions lakeformation:ListPermissions lakeformation:RegisterResource lakeformation:RevokePermissions

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ram:GetResourceShareAssociations ram:GetResourceShares ram:UpdateResourceShare s3:PutObject

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSubscriberNotification	Gewährt die Berechtigung zum Erstellen eines Webhook-Aufrufs, um einen Client zu benachrichtigen, wenn sich neue Daten im Data Lake befinden	Schreiben	subscriber*		events:CreateApiDestination events:CreateConnection events:DescribeRule events:ListApiDestinations events:ListConnections events:PutRule events:PutTargets iam:DeleteRolePolicy iam:GetRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					iam:PassRole s3:GetBucketNotification s3:PutBucketNotification sqs:CreateQueue sqs:DeleteQueue sqs:GetQueueAttributes sqs:GetQueueUrl sqs:SetQueueAttributes

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteAwsLogSource	Gewährt die Berechtigung zum Deaktivieren jedes Quelltyps in einer beliebigen Region für Konten, die Teil einer vertrauenswürdigen Organisation oder eigenständige Konten sind	Schreiben	data-lake*		
DeleteCustomLogSource	Gewährt die Berechtigung zum Entfernen einer benutzerdefinierten Quelle	Schreiben	data-lake*		glue:StopCrawlerSchedule
DeleteDataLake	Gewährt die Berechtigung zum Löschen eines Security Data Lakes	Schreiben	data-lake*		organizations:DescribeOrganization organizations:ListDelegatedAdministrators organizations:ListDelegatedServicesForAccount

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteDataLakeExceptionSubscription	Gewährt die Berechtigung zum Abmelden von SNS-Themen für Ausnahmebenachrichtigungen. Entfernt Ausnahmebenachrichtigungen für das SNS-Thema	Schreiben			
DeleteDataLakeOrganizationConfiguration	Gewährt die Berechtigung zum Entfernen der automatische Aktivierung des Amazon-Security-Lake-Zugriffs für neue Organisationskonten	Schreiben	data-lake*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteSubscriber	Gewährt die Berechtigung zum Löschen des angegebenen Subscribers	Schreiben	subscriber*		events:DeleteApiDestination events:DeleteConnection events:DeleteRule events:DescribeRule events:ListApiDestinations events:ListTargetsByRule events:RemoveTargets iam:DeleteRole iam:DeleteRolePolicy

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					iam:GetRole iam:ListRolePolicies lakeformation:ListPermissions lakeformation:RevokePermissions sqs:DeleteQueue sqs:GetQueueUrl

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteSubscriberNotification	Gewährt die Berechtigung zum Entfernen eines Webhook-Aufrufs, um einen Client zu benachrichtigen, wenn sich neue Daten im Data Lake befinden	Schreiben	subscriber*		events:DeleteApiDestination events:DeleteConnection events:DeleteRule events:DescribeRule events:ListApiDestinations events:ListTargetsByRule events:RemoveTargets iam:DeleteRole iam:DeleteRolePolicy

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					iam:GetRole iam:ListRolePolicies lakeformation:RevokePermissions sqs:DeleteQueue sqs:GetQueueUrl
DeregisterDataLakeDelegatedAdministrator	Gewährt die Berechtigung zum Entfernen des Kontos des delegierten Administrators und zum Deaktivieren von Amazon Security Lake als Service für diese Organisation	Schreiben			organizations:DeregisterDelegatedAdministrator organizations:DescribeOrganization organizations:ListDelegatedServicesForAccount

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDataLakeExceptionSubscription	Gewährt die Berechtigung zum Abfragen des das Protokolls und des Endpunkts, die beim Abonnieren der SNS-Themen für Ausnahmebenachrichtigungen angegeben wurden	Lesen			
GetDataLakeOrganizationConfiguration	Gewährt die Berechtigung zum Abrufen der Konfigurationseinstellung einer Organisation für die automatische Aktivierung des Amazon-Security-Lake-Zugriffs für neue Organisationskonten	Lesen	data-lake*		organizations:DescribeOrganization
GetDataLakeSources	Gewährt die Berechtigung zum Abrufen eines statischen Snapshots des Security Data Lake in der aktuellen Region. Der Snapshot enthält aktivierte Konten und Protokollquellen	Lesen	data-lake*		
GetSubscriber	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Subscriber, der bereits erstellt wurde	Lesen	subscriber*		
ListDataLakeExceptions	Gewährt die Berechtigung zum Abrufen einer Liste aller nicht wiederholbaren Fehler	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDataLakes	Gewährt die Berechtigung zum Auflisten von Informationen zu Security Data Lakes	Auflisten			
ListLogSources	Gewährt die Berechtigung zum Anzeigen der aktivierten Konten. Sie können die aktivierten Quellen in den aktivierten Regionen anzeigen	Auflisten			
ListSubscribers	Gewährt die Berechtigung zum Auflisten aller Subscribers	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten aller Tags für eine Ressource	Auflisten	data-lake		
			subscriber		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RegisterDataLakeDelegatedAdministrator	Gewährt die Berechtigung zum Bestimmen eines Kontos als Amazon-Security-Lake-Administratorkonto für die Organisation	Schreiben			iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators organizations:ListDelegatedServicesForAccount organizations:RegisterDelegatedAdministrator

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zur Ressource	Tagging	data-lake		
			subscriber		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags von der Ressource	Tagging	data-lake		
			subscriber		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateDataLake	Gewährt die Berechtigung zum Aktualisieren eines Security Data Lake	Schreiben	data-lake *		events:PutRule events:PutTargets iam:CreateServiceLinkedRole iam:DeleteRolePolicy iam:GetRole iam:ListAttachedRolePolicies iam:PutRolePolicy kms:CreateGrant kms:DescribeKey lakeformation:GetDataLakeSettings

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					lakeformation:PutDataLakeSettings lambda:AddPermission lambda:CreateEventSourceMapping lambda:CreateFunction organizations:DescribeOrganization organizations:ListDelegatedServicesForAccount s3:CreateBucket s3:GetObject

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					s3:GetObjectVersion s3:ListBucket s3:PutBucketPolicy s3:PutBucketPublicAccessBlock s3:PutBucketVersioning sqs:CreateQueue sqs:GetQueueAttributes sqs:SetQueueAttributes

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateDataLakeExceptionSubscription	Gewährt die Berechtigung zum Aktualisieren von Abonnements für die SNS-Themen für Ausnahmebenachrichtigungen	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateSubscriber	Gewährt die Berechtigung zum Aktualisieren eines Subscribers	Schreiben	subscriber*		events:CreateApiDestination events:CreateConnection events:DescribeRule events:ListApiDestinations events:ListConnections events:PutRule events:PutTargets iam:DeleteRolePolicy iam:GetRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					iam:PutRolePolicy

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateSubscriberNotification	Gewährt die Berechtigung zum Aktualisieren eines Webhook-Aufrufs, um einen Client zu benachrichtigen, wenn sich neue Daten im Data Lake befinden	Schreiben	subscriber*		events:CreateApiDestination events:CreateConnection events:DescribeRule events:ListApiDestinations events:ListConnections events:PutRule events:PutTargets iam:CreateServiceLinkedRole iam:DeleteRolePolicy

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					iam:GetRole iam:PassRole iam:PutRolePolicy s3:CreateBucket s3:GetBucketNotification s3:ListBucket s3:PutBucketNotification s3:PutBucketPolicy s3:PutBucketPublicAccessBlock s3:PutBucketVersioning

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					s3:PutLifecycleConfiguration sqs:CreateQueue sqs:DeleteQueue sqs:GetQueueAttributes sqs:GetQueueUrl sqs:SetQueueAttributes

Von Amazon Security Lake definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
data-lake	`arn:${Partition}:securitylake:${Region}:${Account}:data-lake/default`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}
subscriber	`arn:${Partition}:securitylake:${Region}:${Account}:subscriber/${SubscriberId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Security Lake

Amazon Security Lake definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch Tags, die in der Anforderung übergeben werden	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paar einer Ressource	String
aws:TagKeys	Filtert den Zugriff basierend auf Tag-Schlüsseln, die in der Anforderung übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Security Token Service

AWS Der Security Token Service (Dienstpräfix:`sts`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Security Token Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie

den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssumeRole	Erteilt die Berechtigung zum Abrufen einer Reihe temporärer Sicherheitsanmeldedaten, mit denen Sie auf AWS Ressourcen zugreifen können, auf die Sie normalerweise keinen Zugriff haben	Schreiben	role*		
				aws:TagKeys aws:RequestTag/${TagKey} sts:TransitiveTagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				sts:ExternalId sts:RoleSessionName iam:ResourceTag/${TagKey} sts:SourceIdentity cognito-identity.amazonaws.com:amr cognito-identity.amazonaws.com:aud cognito-identity.amazonaws.com:sub www.amazon.com:app_id	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				www.amazon.com:user_id graph.facebook.com:app_id graph.facebook.com:id accounts.google.com:aud accounts.google.com:sub saml:namequalifier saml:sub saml:sub_type	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssumeRoleWithSAML	Gewährt die Berechtigung, einen Satz temporärer Sicherheits-Anmeldeinformationen für Benutzer abzurufen, die mittels SAML-Authentifizierungsantwort authentifiziert wurden	Schreiben	role*	saml:namequalifier saml:sub saml:sub_type saml:aud saml:iss saml:doc saml:cn saml:commonName saml:eduorghomepageuri saml:eduorgidentityauthnpolicyuri saml:eduorglegalname	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				saml:eduorgsuperioruri saml:eduorgwhitepagesuri saml:edupersonaffiliation saml:edupersonassurance saml:edupersonentitlement saml:edupersonnickname saml:edupersonorgdn saml:edupersonorgunitdn saml:edupersonprim	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aryaffiliation saml:edupersonprimaryorgunitdn saml:edupersonprincipalname saml:edupersonscopedaffiliation saml:edupersontargetedid saml:givenName saml:mail saml:name saml:organizationStatus saml:primaryGroupSID	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				saml:surname saml:uid saml:x500UniqueIdentifier aws:TagKeys aws:RequestTag/${TagKey} sts:TransitiveTagKeys sts:SourceIdentity sts:RoleSessionName	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssumeRoleWithWebIdentity	Gewährt die Berechtigung, einen Satz temporärer Sicherheits-Anmeldeinformationen für Benutzer abzurufen, die in einer mobilen App oder Webanwendung mit einem Web-Identitätsanbieter authentifiziert wurden	Schreiben	role*		
				cognito-identity.amazonaws.com:amr cognito-identity.amazonaws.com:aud cognito-identity.amazonaws.com:sub www.amazon.com:app_id www.amazon.com:user_id graph.facebook.com:app_id graph.facebook.com:id	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				accounts.google.com:aud accounts.google.com:oaud accounts.google.com:sub aws:TagKeys aws:RequestTag/${TagKey} sts:TransitiveTagKeys sts:SourceIdentity sts:RoleSessionName	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DecodeAuthorizationMessage	Erteilt die Berechtigung, zusätzliche Informationen über den Autorisierungsstatus einer Anfrage aus einer codierten Nachricht zu dekodieren, die als Antwort auf eine Anfrage zurückgegeben wird AWS	Schreiben			
GetAccessKeyInfo	Gewährt die Berechtigung zum Abrufen von Details über die Zugriffsschlüssel-ID, die als Parameter an die Anforderung übergeben wurde	Lesen			
GetCallerIdentity	Gewährt die Berechtigung zum Abrufen von Details über die IAM-Identität, deren Anmeldeinformationen zum Aufrufen der API verwendet wurden	Lesen			
GetFederationToken	Gewährt die Berechtigung, einen Satz temporärer Sicherheits-Anmeldeinformationen (bestehend aus Zugriffsschlüssel-ID, geheimem Zugriffsschlüssel und Sicherheits-Token) für einen verbundenen Benutzer abzurufen	Lesen	user		
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetServiceBearerToken [nur Berechtigung]	Erteilt die Berechtigung zum Abrufen eines STS-Bearer-Tokens für einen AWS Root-Benutzer, eine IAM-Rolle oder einen IAM-Benutzer	Lesen		sts:AWSServiceName sts:DurationSeconds	
GetSessionToken	Erteilt die Berechtigung zum Abrufen eines Satzes temporärer Sicherheitsanmeldeinformationen (bestehend aus einer Zugriffsschlüssel-ID, einem geheimen Zugriffsschlüssel und einem Sicherheitstoken) für einen AWS-Konto oder IAM-Benutzer	Lesen			
SetContext [nur Berechtigung]	Gewährt die Berechtigung, Kontextschlüssel für eine STS-Sitzung festzulegen	Schreiben	role		
			self-session		
				sts:RequestContext/${ContextKey} sts:RequestContextProviders	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SetSourceIdentity [nur Berechtigung]	Gewährt die Berechtigung, eine Quellenidentität für eine STS-Sitzung festzulegen	Write	role		
			user		
				sts:SourceIdentity	
TagSession [nur Berechtigung]	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer STS-Sitzung.	Markieren	role		
			user		
				aws:TagKeys aws:RequestTag/${TagKey} sts:TransitiveTagKeys saml:aud	

Vom AWS Security Token Service definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
role	`arn:${Partition}:iam::${Account}:role/${RoleNameWithPath}`	aws:ResourceTag/${TagKey} iam:ResourceTag/${TagKey}
user	`arn:${Partition}:iam::${Account}:user/${UserNameWithPath}`	
self-session	`arn:${Partition}:sts::${Account}:self`	

Bedingungsschlüssel für AWS Security Token Service

AWS Der Security Token Service definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
accounts.google.com:aud	Filtert den Zugriff nach der Google-Anwendungs-ID	String
accounts.google.com:oaud	Filtert den Zugriff nach der Google-Zielgruppe	String
accounts.google.com:sub	Filtert den Zugriff nach dem Gegenstand des Antrags (die ID des Google-Benutzers)	String
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString
cognito-identity.amazonaws.com:amr	Filtert den Zugriff nach den Anmeldeinformationen für Amazon Cognito	String
cognito-identity.amazonaws.com:aud	Filtert den Zugriff nach der ID des Amazon-Cognito-Identitäten-Pools	String
cognito-identity.amazonaws.com:sub	Filtert den Zugriff nach dem Gegenstand des Antrags (der ID des Amazon-Cognito-Benutzers)	String
graph.facebook.com:app_id	Filtert den Zugriff nach der ID der Facebook-Anwendung	String
graph.facebook.com:id	Filtert den Zugriff nach der ID des Facebook-Benutzers	String
iam:ResourceTag/${TagKey}	Filtert den Zugriff nach den Tags, die der Rolle zugeordnet sind, die angenommen wird	String
saml:aud	Filtert den Zugriff nach der Endpunkt-URL, für die SAML-Zusicherungen angezeigt werden	String

Bedingungsschlüssel	Beschreibung	Typ
saml:cn	Filtert Zugriff nach dem eduOrg-Attribut	ArrayOfString
saml:commonName	Filtert den Zugriff nach dem commonName-Attribut	String
saml:doc	Filtert den Zugriff nachdem Prinzipal, der zum Übernehmen der Rolle verwendet wurde	String
saml:eduorghomepageuri	Filtert Zugriff nach dem eduOrg-Attribut	ArrayOfString
saml:eduorgidentityauthnpolicyuri	Filtert Zugriff nach dem eduOrg-Attribut	ArrayOfString
saml:eduorglegalname	Filtert Zugriff nach dem eduOrg-Attribut	ArrayOfString
saml:eduorgsuperioruri	Filtert Zugriff nach dem eduOrg-Attribut	ArrayOfString
saml:eduorgwhitepagesuri	Filtert Zugriff nach dem eduOrg-Attribut	ArrayOfString
saml:edupersonaffiliation	Filtert Zugriff nach dem eduPerson-Attribut	ArrayOfString
saml:edupersonassurance	Filtert Zugriff nach dem eduPerson-Attribut	ArrayOfString
saml:edupersonentitlement	Filtert Zugriff nach dem eduPerson-Attribut	ArrayOfString
saml:edupersonnickname	Filtert Zugriff nach dem eduPerson-Attribut	ArrayOfString

Bedingungsschlüssel	Beschreibung	Typ
saml:edupersonorgdn	Filtert Zugriff nach dem eduPerson-Attribut	String
saml:edupersonorgunitdn	Filtert Zugriff nach dem eduPerson-Attribut	ArrayOfString
saml:edupersonprimaryaffiliation	Filtert Zugriff nach dem eduPerson-Attribut	String
saml:edupersonprimaryorgunitdn	Filtert Zugriff nach dem eduPerson-Attribut	String
saml:edupersonprincipalname	Filtert Zugriff nach dem eduPerson-Attribut	String
saml:edupersonscopedaffiliation	Filtert Zugriff nach dem eduPerson-Attribut	ArrayOfString
saml:edupersontargetedid	Filtert Zugriff nach dem eduPerson-Attribut	ArrayOfString
saml:givenName	Filtert den Zugriff nach dem givenName-Attribut	String
saml:iss	Filtert den Zugriff nach dem Aussteller, der durch einen URN dargestellt wird	String
saml:mail	Filtert den Zugriff nach dem mail-Attribut	String
saml:name	Filtert den Zugriff nach dem name-Attribut	String

Bedingungsschlüssel	Beschreibung	Typ
saml:namequalifier	Filtert den Zugriff nach dem Hash-Wert des Ausstellers, der Konto-ID und dem Anzeigenamen	String
saml:organizationStatus	Filtert den Zugriff nach dem organizationStatus-Attribut	String
saml:primaryGroupSID	Filtert den Zugriff nach dem primaryGroupSID-Attribut	String
saml:sub	Filtert den Zugriff nach dem Gegenstand des Antrags (die ID des SAML-Benutzers)	String
saml:sub_type	Filtert den Zugriff nach dem Wert „persistent“, „transient“ oder dem vollständigen Format-URI	String
saml:surname	Filtert den Zugriff nach dem surname-Attribut	String
saml:uid	Filtert den Zugriff nach dem uid-Attribut	String
saml:x500UniqueIdentifier	Filtert den Zugriff nach dem uid-Attribut	String
sts:AWSServiceName	Filtert den Zugriff nach dem Service, der ein Inhaber-Token erhält	String
sts:DurationSeconds	Filtert den Zugriff nach der Dauer in Sekunden, wenn ein Inhaber-Token abgerufen wird	String
sts:ExternalId	Filtert den Zugriff nach der eindeutigen Kennung, die erforderlich ist, wenn Sie eine Rolle in einem anderen Konto übernehmen	String
sts:RequestContext/${ContextKey}	Filtert den Zugriff anhand der Schlüssel-Wert-Paare aus dem Sitzungskontext, eingebettet in die signierte Kontext-Assertion, die von einem vertrauenswürdigen Kontextanbieter abgerufen wurde	String

Bedingungsschlüssel	Beschreibung	Typ
sts:RequestContextProviders	Filtert den Zugriff nach Context-Provider-ARNs	ArrayOfARN
sts:RoleSessionName	Filtert den Zugriff nach dem Namen der Rollensitzung, der erforderlich ist, wenn Sie eine Rolle übernehmen	String
sts:SourceIdentity	Filtert den Zugriff nach der Quellenidentität, die in der Anfrage übergeben wird	String
sts:TransitiveTagKeys	Filtert den Zugriff nach den transitiven Tag-Schlüsseln, die in der Anforderung übergeben werden	ArrayOfString
www.amazon.com:app_id	Filtert den Zugriff nach der Anwendungs-ID von Login with Amazon	String
www.amazon.com:user_id	Filtert den Zugriff nach der Benutzer-ID von Login with Amazon	String

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Server Migration Service

AWS Server Migration Service (Servicepräfix: `sms`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Server Migration Service definierte Aktionen
- Von AWS Server Migration Service definierte Ressourcentypen
- Bedingungsschlüssel für AWS Server Migration Service

Von AWS Server Migration Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateApp	Gewährt die Berechtigung zum Erstellen einer Anwendungskonfiguration zum Migrieren von lokalen Anwendungen zu AWS	Write			
CreateReplicationJob	Gewährt die Berechtigung zum Erstellen einer Aufgabe zum Migrieren von On-Premise-Servern zu AWS	Write			
DeleteApp	Gewährt die Berechtigung zum Löschen einer vorhandenen Anwendungskonfiguration	Write			
DeleteAppLaunchConfiguration	Gewährt die Berechtigung zum Löschen der Startkonfiguration für eine vorhandene Anwendung	Write			
DeleteAppReplicationConfiguration	Gewährt die Berechtigung zum Löschen der Replikationskonfiguration für eine vorhandene Anwendung	Write			
DeleteAppValidationConfiguration	Gewährt die Berechtigung zum Löschen der Validierungskonfiguration für eine vorhandene Anwendung	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteReplicationJob	Gewährt die Berechtigung zum Löschen einer vorhandenen Aufgabe zum Migrieren des On-Premise-Servers zu AWS	Write			
DeleteServerCatalog	Gewährt die Berechtigung zum Löschen der vollständigen Liste der lokal installierten Server, die in AWS gesammelt werden	Write			
DisassociateConnector	Gewährt die Berechtigung zum Aufheben der Mapping eines zugeordneten Connectors	Write			
GenerateChangeSet	Gewährt die Berechtigung zum Erstellen eines changeSet für den CloudFormation-Stack einer Anwendung.	Write			
GenerateTemplate	Gewährt die Berechtigung zum Generieren einer CloudFormation-Vorlage für eine vorhandene Anwendung	Write			
GetApp	Gewährt die Berechtigung zum Abrufen der Konfiguration und des Status einer vorhandenen Anwendung	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAppLaunchConfiguration	Gewährt die Berechtigung zum Abrufen der Startkonfiguration für eine vorhandene Anwendung	Read			
GetAppReplicationConfiguration	Gewährt die Berechtigung zum Abrufen der Replikationskonfiguration für eine vorhandene Anwendung	Read			
GetAppValidationConfiguration	Gewährt die Berechtigung zum Abrufen der Validierungskonfiguration für eine vorhandene Anwendung	Read			
GetAppValidationOutput	Gewährt die Berechtigung zum Abrufen von Benachrichtigungen, die vom Anwendungsvalidierungsskript gesendet werden.	Read			
GetConnectors	Gewährt die Berechtigung, alle zugeordneten Connectors abzurufen.	Read			
GetMessages [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Nachrichten vom AWS Server Migration Service an den Server Migration Connector	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetReplicationJobs	Gewährt die Berechtigung, alle vorhandenen Aufgaben für die Migrierung von lokalen Servern zu AWS abzurufen	Read			
GetReplicationRuns	Gewährt die Berechtigung zum Abrufen aller Runs für eine vorhandene Aufgabe.	Read			
GetServers	Gewährt die Berechtigung zum Abrufen aller importierten Server.	Read			
ImportAppCatalog	Gewährt die Berechtigung zum Importieren des Anwendungskatalogs aus AWS Application Discovery Service	Write			
ImportServerCatalog	Gewährt die Berechtigung zum Sammeln einer vollständigen Liste der lokalen Server	Write			
LaunchApp	Gewährt die Berechtigung zum Erstellen und Starten eines ClouFormation-Stacks für eine vorhandene Anwendung.	Write			
ListApps	Gewährt die Berechtigung zum Abrufen einer Liste von Zusammenfassungen für vorhandene Anwendungen	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
NotifyAppValidationOutput	Gewährt die Berechtigung zum Senden von Benachrichtigungen für ein Anwendungsvalidierungsskript	Write			
PutAppLaunchConfiguration	Gewährt die Berechtigung zum Erstellen oder Aktualisieren einer Startkonfiguration für eine vorhandene Anwendung	Write			
PutAppReplicationConfiguration	Gewährt die Berechtigung zum Erstellen oder Aktualisieren einer Replikationskonfiguration für eine vorhandene Anwendung	Write			
PutAppValidationConfiguration	Gewährt die Berechtigung zum Setzen der Validierungskonfiguration für eine vorhandene Anwendung	Write			
SendMessage [nur Berechtigung]	Gewährt die Berechtigung zum Senden einer Nachricht vom Server Migration Connector an den AWS Server Migration Service	Write			
StartAppReplication	Gewährt die Berechtigung zum Erstellen und Starten von Replikationsaufgaben für eine vorhandene Anwendung	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartOnDemandAppReplication	Gewährt die Berechtigung zum Starten eines Replikationsdurchlaufs für eine vorhandene Anwendung	Write			
StartOnDemandReplicationRun	Gewährt die Berechtigung zum Starten eines Replikationsdurchlaufs für eine vorhandene Replikationsaufgabe	Write			
StopAppReplication	Gewährt die Berechtigung zum Beenden und Löschen von Replikationsaufgaben für eine vorhandene Anwendung	Write			
TerminateApp	Gewährt die Berechtigung zum Beenden des CloudFormation-Stacks für eine vorhandene Anwendung	Write			
UpdateApp	Gewährt die Berechtigung zum Aktualisieren einer vorhandenen Anwendungskonfiguration	Write			
UpdateReplicationJob	Gewährt die Berechtigung zum Aktualisieren einer vorhandenen Aufgabe zur Migrierung von On-Premise-Servern zu AWS	Write			

Von AWS Server Migration Service definierte Ressourcentypen

AWS Server Migration Service unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf AWS Server Migration Service zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Server Migration Service

Server Migration Service umfasst keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Serverless Application Repository

AWS Serverless Application Repository (Servicepräfix: `serverlessrepo`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Serverless Application Repository definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen.

Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateApplication	Erstellt eine Anwendung, optional mit einer AWS SAM-Datei, damit die erste Anwendungsversion im selben Aufruf erstellt wird	Schreiben			
CreateApplicationVersion	Gewährt die Berechtigung zum Erstellen einer Anwendungsversion	Schreiben	applications*		
CreateCloudFormationChangeSet	Erteilt die Berechtigung zum Erstellen eines AWS CloudFormation ChangeSet für die angegebene Anwendung	Schreiben	applications*		
				serverlessrepo:applicationType	
CreateCloudFormationTemplate	Gewährt die Berechtigung zum Erstellen einer AWS-CloudFormation-Vorlage	Schreiben	applications*		
				serverlessrepo:applicationType	
DeleteApplication	Gewährt die Berechtigung zum Löschen der angegebenen Anwendung	Schreiben	applications*		
GetApplication	Gewährt die Berechtigung zum Abrufen der angegebenen Anwendung	Lesen	applications*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				serverlessrepo:applicationType	
GetApplicationPolicy	Erteilt die Berechtigung zum Abrufen der Richtlinie für die angegebene Anwendung	Lesen	applications*		
GetCloudFormationTemplate	Erteilt die Berechtigung zum Abrufen der angegebenen AWS-CloudFormation-Vorlage	Lesen	applications*		
ListApplicationDependencies	Erteilt die Berechtigung zum Abrufen der Liste der Anwendungen, die in der enthaltenden Anwendung verschachtelt sind	Auflisten	applications*		
				serverlessrepo:applicationType	
ListApplicationVersions	Erteilt die Berechtigung zum Auflisten von Versionen für die angegebene Anwendung, die dem Anforderer gehört	Auflisten	applications*		
				serverlessrepo:applicationType	
ListApplications	Erteilt die Berechtigung zum Auflisten von Anwendungen, die dem Anforderer gehören	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutApplicationPolicy	Erteilt die Berechtigung zum Festlegen der Richtlinie für die angegebene Anwendung	Schreiben	applications*		
SearchApplications	Erteilt die Berechtigung, alle Anwendungen für diesen Benutzer zu autorisieren	Lesen		serverlessrepo:applicationType	
UnshareApplication	Erteilt die Berechtigung zum Aufheben der Freigabe der angegebenen Anwendung	Schreiben	applications*		
UpdateApplication	Erteilt die Berechtigung zum Aktualisieren von Metadaten der Anwendung	Schreiben	applications*		

Von AWS Serverless Application Repository definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
applications	`arn:${Partition}:serverlessrepo:${Region}:${Account}:applications/${ResourceId}`	

Bedingungsschlüssel für AWS Serverless Application Repository

AWS Serverless Application Repository definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
serverlessrepo:applicationType	Filtert den Zugriff nach Anwendungstyp	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Service Catalog

AWS Service Catalog (Servicepräfix: `servicecatalog`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Service Catalog definierte Aktionen
- Von AWS Service Catalog definierte Ressourcentypen
- Bedingungsschlüssel für AWS Service Catalog

Von AWS Service Catalog definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptPortfolioShare	Gewährt die Berechtigung, ein Portfolio anzunehmen, das für Sie freigegeben wurde	Write	Portfolio*		
AssociateAttributeGroup	Gewährt die Berechtigung, einer Anwendung eine Attributgruppe zuzuordnen	Write	Application* AttributeGroup*		
AssociateBudgetWithResource	Gewährt die Berechtigung, ein Budget mit einer Ressource zu verknüpfen	Write			
AssociatePrincipalWithPortfolio	Gewährt die Berechtigung, einen IAM-Prinzipal einem Portfolio zuzuordnen, damit der angegebene Prinzipal Zugriff auf alle Produkte erhält, die dem angegebenen Portfolio zugeordnet sind	Write	Portfolio*		
AssociateProductWithPortfolio	Gewährt die Berechtigung, ein Produkt mit einem Portfolio zu verknüpfen	Write			
AssociateResource	Gewährt die Berechtigung, einer Anwendung eine Ressource zuzuordnen	Write	Application*		cloudformation:DescribeStacks resource-groups:Cr

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					eateGroup resource-groups:GetGroup resource-groups:Tag
				servicecatalog:ResourceType servicecatalog:Resource	
AssociateServiceActionWithProvisioningArtifact	Gewährt die Berechtigung zum Zuordnen einer Aktion zu einem Bereitstellungsartefakt	Write	Product*		
AssociateTagOptionWithResource	Gewährt die Berechtigung, die angegebene TagOption mit dem angegebenen Portfolio oder Produkt zu verknüpfen	Write	Portfolio Product		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchAssociateServiceActionWithProvisioningArtifact	Gewährt die Berechtigung zum Zuordnen mehrerer Self-Service-Aktionen zu Bereitstellungsartefakten	Write			
BatchDisassociateServiceActionFromProvisioningArtifact	Gewährt die Berechtigung, die Mapping eines Batch von Self-Service-Aktionen zu dem angegebenen Bereitstellungsartefakt aufzuheben	Write			
CopyProduct	Gewährt die Berechtigung, das angegebene Quellprodukt in das angegebene Zielprodukt oder ein neues Produkt zu kopieren	Write			
CreateApplication	Gewährt die Berechtigung zum Erstellen einer Anwendung	Write	Application*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAttributeGroup	Gewährt die Berechtigung zum Erstellen einer Attributgruppe	Write	AttributeGroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConstraint	Gewährt die Berechtigung zum Erstellen einer Einschränkung für ein zugeordnetes Produkt und Portfolio	Write	Product*		
CreatePortfolio	Gewährt die Berechtigung zum Erstellen eines Portfolios	Write	Portfolio*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePortfolioShare	Gewährt die Berechtigung, ein Portfolio in Ihrem Besitz mit einem anderen AWS-Konto zu teilen	Berechtigungsverwaltung	Portfolio*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateProduct	Gewährt die Berechtigung zum Erstellen eines Produkts und des ersten Bereitstellungs-Artefakts dieses Produkts	Write	Product*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProvisionedProductPlan	Gewährt die Berechtigung zum Hinzufügen eines neuen bereitgestellten Produktplans	Write		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
CreateProvisioningArtifact	Gewährt die Berechtigung zum Hinzufügen eines neuen Bereitstellungsartefakts zu einem vorhandenen Produkt	Write	Product*		
CreateServiceAction	Gewährt die Berechtigung zum Erstellen einer Self-Service-Aktion	Write			
CreateTagOption	Gewährt die Berechtigung zum Erstellen einer TagOption	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteApplication	Gewährt die Berechtigung zum Löschen einer Anwendung, wenn alle Mappings aus der Anwendung entfernt wurden	Write	Application*		
DeleteAttributeGroup	Gewährt die Berechtigung zum Löschen einer Attributgruppe, wenn alle Mappings aus der Attributgruppe entfernt wurden	Write	AttributeGroup*		
DeleteConstraint	Gewährt die Berechtigung zum Entfernen und Löschen einer vorhandenen Einschränkung aus einem zugeordneten Produkt und Portfolio	Write			
DeletePortfolio	Gewährt die Berechtigung zum Löschen eines Portfolios, wenn alle Mappings und Freigaben aus dem Portfolio entfernt wurden	Write	Portfolio*		
DeletePortfolioShare	Gewährt die Berechtigung zum Aufheben der Freigabe eines Portfolios in Ihrem Besitz für ein AWS-Konto	Berechtigungsverwaltung	Portfolio*		
DeleteProduct	Gewährt die Berechtigung zum Löschen eines Produkts, wenn alle Mappings aus dem Produkt entfernt wurden	Write	Product*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteProvisionedProductPlan	Gewährt die Berechtigung zum Löschen eines bereitgestellten Produktplans	Write		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DeleteProvisioningArtifact	Gewährt die Berechtigung zum Löschen eines Bereitstellungsartefakts aus einem Produkt	Write	Product*		
DeleteServiceAction	Gewährt die Berechtigung zum Löschen einer Self-Service-Aktion	Write			
DeleteTagOption	Gewährt die Berechtigung zum Löschen der angegebenen TagOption	Write			
DescribeConstraint	Gewährt die Berechtigung zum Beschreiben einer Einschränkung	Read			
DescribeCopyProductStatus	Gewährt die Berechtigung, den Status des angegebenen Produktion zum Kopieren des Produkts abzurufen	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribePortfolio	Gewährt die Berechtigung zum Beschreiben eines Portfolios	Read	Portfolio*		
DescribePortfolioShareStatus	Gewährt die Berechtigung, den Status der angegebenen Produktion zum Freigeben des Portfolios abzurufen	Read			
DescribePortfolioShares	Gewährt die Berechtigung zum Anzeigen einer Zusammenfassung der einzelnen Portfolioaktien, die für das angegebene Portfolio erstellt wurden	List	Portfolio*		
DescribeProduct	Gewährt die Berechtigung, ein Produkt als Endbenutzer zu beschreiben	Read	Product*		
DescribeProductAsAdmin	Gewährt die Berechtigung, ein Produkt als Administrator zu beschreiben	Read	Product*		
DescribeProductView	Gewährt die Berechtigung, ein Produkt als Endbenutzer zu beschreiben	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeProvisionedProduct	Gewährt die Berechtigung, ein bereitgestelltes Produkt zu beschreiben	Read		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DescribeProvisionedProductPlan	Gewährt die Berechtigung zum Beschreiben eines bereitgestellten Produktplans	Read		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DescribeProvisioningArtifact	Gewährt die Berechtigung zum Beschreiben eines Bereitstellungsartefakts	Read	Product*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeProvisioningParameters	Gewährt die Berechtigung zur Beschreibung der Parameter, die Sie angeben müssen, um ein angegebenes Bereitstellungsartefakt erfolgreich bereitzustellen	Read	Product*		
DescribeRecord	Gewährt die Berechtigung zur Beschreibung eines Datensatzes und listet alle Ausgaben auf	Read		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DescribeServiceAction	Gewährt die Berechtigung zur Beschreibung einer Self-Service-Aktion	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeServiceActionExecutionParameters	Gewährt die Berechtigung zum Abrufen der Standardparameter, wenn Sie die angegebene Service-Aktion für das angegebene bereitgestellte Produkt ausgeführt haben.	Read		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DescribeTagOption	Gewährt die Berechtigung zum Abrufen von Informationen über die angegebene TagOption	Read			
DisableAWSOrganizationsAccess	Gewährt die Berechtigung zum Deaktivieren der Portfoliofreigabe über die AWS-Organizations-Funktion	Write			
DisassociateAttributeGroup	Gewährt die Berechtigung, die Mapping einer Attributgruppe zu einer Anwendung zu trennen	Write	Application* AttributeGroup*		
DisassociateBudgetFromResource	Gewährt die Berechtigung, ein Budget von einer Ressource zu trennen	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociatePrincipalFromPortfolio	Gewährt die Berechtigung, die Mapping eines IAM-Prinzipals zu einem Portfolio aufzuheben	Write	Portfolio*		
DisassociateProductFromPortfolio	Gewährt die Berechtigung, die Mapping eines Produkts zu einem Portfolio aufzuheben	Write			
DisassociateResource	Gewährt die Berechtigung, die Mapping einer Ressource zu einer Anwendung zu trennen	Write	Application*		resource-groups:DeleteGroup
				servicecatalog:ResourceType servicecatalog:Resource	
DisassociateServiceActionFromProvisioningArtifact	Gewährt die Berechtigung zum Aufheben der Mapping der angegebenen Self-Service-Aktion zum angegebenen Bereitstellungsartefakt.	Write	Product*		
DisassociateTagOptionFromResource	Gewährt die Berechtigung, die Mapping der angegebenen TagOption zur angegebenen Ressource aufzuheben	Write	Portfolio Product		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
EnableAWSOrganizationsAccess	Gewährt die Berechtigung zum Aktivieren der Portfolio-Freigabefunktion über AWS Organizations	Write			
ExecuteProvisionedProductPlan	Gewährt die Berechtigung zum Ausführen eines bereitgestellten Produktplans	Write		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ExecuteProvisionedProductServiceAction	Gewährt die Berechtigung zum Ausführen eines bereitgestellten Produktplans	Write		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAWSOrganizationsAccessStatus	Gewährt die Berechtigung zum Abrufen des Zugriffsstatus für die Portfolio-Freigabefunktion von AWS Organizations	Read			
GetApplication	Gewährt die Berechtigung zum Abrufen einer Anwendung	Read	Application*		
GetAssociatedResource	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Anwendung	Read	Application*		
				servicecatalog:ResourceType servicecatalog:Resource	
GetAttributeGroup	Gewährt die Berechtigung zum Abrufen einer Attributgruppe	Lesen	AttributeGroup*		
GetConfiguration	Gewährt die Berechtigung zum Lesen von AppRegistry-Konfigurationen	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetProvisionedProductOutputs	Gewährt die Berechtigung, die bereitgestellte Produktausgabe entweder mit einer bereitgestellten Produkt-ID oder einem Namen zu erhalten	Read			
ImportAsProvisionedProduct	Gewährt die Berechtigung zum Importieren einer Ressource in ein bereitgestelltes Produkt	Write	Product*		
ListAcceptedPortfolioShares	Gewährt die Berechtigung, die Portfolios aufzulisten, die für Sie freigegeben wurden und die Sie akzeptiert haben	Auflisten			
ListApplications	Gewährt die Berechtigung zum Auflisten Ihrer Anwendungen	Auflisten			
ListAssociatedAttributeGroups	Gewährt die Berechtigung, die einer Anwendung zugeordneten Attributgruppen aufzulisten	List	Application*		
ListAssociatedResources	Gewährt die Berechtigung, die einer Anwendung zugeordneten Ressourcen aufzulisten	Auflisten	Application*		
ListAttributeGroups	Gewährt die Berechtigung zum Auflisten Ihrer Attributgruppen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAttributeGroupsForApplication	Gewährt die Berechtigung zum Auflisten der zugeordneten Attributgruppen einer vorgegebenen Anwendung	Auflisten	Application*		
ListBudgetsForResource	Gewährt die Berechtigung zum Auflisten aller Budgets, die einer Ressource zugeordnet sind	List			
ListConstraintsForPortfolio	Gewährt die Berechtigung zum Auflisten von Einschränkungen, die mit einem bestimmten Portfolio verknüpft sind	List			
ListLaunchPaths	Gewährt die Berechtigung, die verschiedenen Möglichkeiten zur Einführung eines bestimmten Produkts als Endbenutzer aufzulisten	List	Product*		
ListOrganizationPortfolioAccess	Gewährt die Berechtigung zum Auflisten der Organisationsknoten, die Zugriff auf das angegebene Portfolio haben	List			
ListPortfolioAccess	Gewährt die Berechtigung zum Auflisten der AWS-Konten, für die Sie ein bestimmtes Portfolio freigegeben haben	List	Portfolio*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListPortfolios	Gewährt die Berechtigung, die Portfolios in Ihrem Konto aufzulisten	List			
ListPortfoliosForProduct	Gewährt die Berechtigung zum Auflisten der Portfolios, die mit einem bestimmten Produkt verknüpft sind	List	Product*		
ListPrincipalsForPortfolio	Gewährt die Berechtigung zum Auflisten der IAM-Prinzipale, die einem bestimmten Portfolio zugeordnet sind	List	Portfolio*		
ListProvisionedProductPlans	Gewährt die Berechtigung zum Auflisten der bereitgestellten Produktpläne	List		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ListProvisioningArtifacts	Gewährt die Berechtigung zum Auflisten der Bereitstellungsartefakte, die einem bestimmten Produkt zugeordnet sind	List	Product*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListProvisioningArtifactsForServiceAction	Gewährt die Berechtigung zum Auflisten aller Bereitstellungsartefakte für die angegebene Self-Service-Aktion	List			
ListRecordHistory	Gewährt die Berechtigung zum Auflisten aller Datensätze in Ihrem Konto oder aller Datensätze zu einem bestimmten bereitgestellten Produkt	List		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ListResourcesForTagOption	Gewährt die Berechtigung zum Auflisten der Ressourcen, die mit der angegebenen TagOption verknüpft sind	List			
ListServiceActions	Gewährt die Berechtigung zum Auflisten aller Self-Service-Aktionen	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListServiceActionsForProvisioningArtifact	Gewährt die Berechtigung zum Auflisten aller Serviceaktionen, die dem angegebenen Bereitstellungsartefakt in Ihrem Konto zugeordnet sind	List	Product*		
				servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ListStackInstancesForProvisionedProduct	Gewährt die Berechtigung zum Auflisten von Konto, Region und Status der einzelnen Stack-Instances, die einem bereitgestellten Produkt vom Typ CFN_STACKSET zugeordnet sind	List		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ListTagOptions	Gewährt die Berechtigung zum Auflisten der angegebenen TagOptions oder aller TagOptions	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für eine Service-Catalog-Appregistry-Ressource	Lesen	Application		
			AttributeGroup		
NotifyProvisionProductEngineWorkflowResult	Gewährt die Berechtigung, das Ergebnis der Ausführung der Bereitstellungs-Engine mitzuteilen	Schreiben			
NotifyTerminateProvisionedProductEngineWorkflowResult	Gewährt die Berechtigung, das Ergebnis der Ausführung der Terminierungs-Engine mitzuteilen	Schreiben			
NotifyUpdateProvisionedProductEngineWorkflowResult	Gewährt die Berechtigung, das Ergebnis der Ausführung der Aktualisierungs-Engine mitzuteilen	Schreiben			
ProvisionProduct	Gewährt die Berechtigung, ein Produkt mit einem angegebenen Bereitstellungsartefakt und Startparametern bereitzustellen	Schreiben	Product*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutConfiguration	Gewährt die Berechtigung zum Zuweisen der AppRegistry-Konfigurationen	Schreiben			
RejectPortfolioShare	Gewährt die Berechtigung zum Ablehnen eines Portfolios, das für Sie freigegeben wurde, das Sie zuvor akzeptiert haben	Write	Portfolio*		
ScanProvisionedProducts	Gewährt die Berechtigung, alle bereitgestellten Produkte in Ihrem Konto aufzulisten	List		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
SearchProducts	Gewährt die Berechtigung, die Produkte anzubieten, die Ihnen als Endbenutzer zur Verfügung stehen	List			
SearchProductsAsAdmin	Gewährt die Berechtigung zum Auflisten aller Produkte im Konto oder aller Produkte, die einem gegebenen Portfolio zugeordnet sind	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SearchProvisionedProducts	Gewährt die Berechtigung, alle bereitgestellten Produkte in Ihrem Konto aufzulisten	List		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
SyncResource	Gewährt die Berechtigung, eine Ressource mit ihrem aktuellen Status in AppRegistry zu synchronisieren	Write			cloudformation:UpdateStack
TagResource	Gewährt die Berechtigung zum Markieren einer Service-Catalog-Appregistry-Ressource	Markieren	Application		
			AttributeGroup		
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TerminateProvisionedProduct	Gewährt die Berechtigung, ein vorhandenes bereitgestelltes Produkt zu beenden	Write		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
UntagResource	Gewährt die Berechtigung zum Entfernen eines Tags aus einer Service-Catalog-Appregistry-Ressource	Markieren	Application		
			AttributeGroup		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateApplication	Gewährt die Berechtigung zum Aktualisieren der Attribute einer vorhandenen Anwendung	Write	Application*		iam:CreateServiceLinkedRole
UpdateAttributeGroup	Gewährt die Berechtigung zum Aktualisieren der Attribute einer vorhandenen Attributgruppe	Write	AttributeGroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateConstraint	Gewährt die Berechtigung zum Aktualisieren der Metadatenfelder einer vorhandenen Einschränkung	Write			
UpdatePortfolio	Gewährt die Berechtigung zum Aktualisieren der Metadatenfelder und/oder Tags eines vorhandenen Portfolios	Write	Portfolio*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdatePortfolioShare	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren der Ressourcenfreigabe für eine bestehende Portfolio freigabe	Berechtigungsverwaltung	Portfolio*		
UpdateProduct	Gewährt die Berechtigung zum Aktualisieren der Metadatenfelder und/oder Tags eines vorhandenen Produkts	Write	Product*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateProvisionedProduct	Gewährt die Berechtigung zum Aktualisieren eines vorhandenen bereitgestellten Produkts	Write		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
UpdateProvisionedProductProperties	Gewährt die Berechtigung zum Aktualisieren der Eigenschaften eines vorhandenen bereitgestellten Produkts	Write			
UpdateProvisioningArtifact	Gewährt die Berechtigung zum Aktualisieren der Metadatenfelder eines vorhandenen Bereitstellungsartefakts	Write	Product*		
UpdateServiceAction	Gewährt die Berechtigung zur Aktualisierung einer Self-Service-Aktion	Write			
UpdateTagOption	Gewährt die Berechtigung, die angegebene TagOption zu aktualisieren.	Write			

Von AWS Service Catalog definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Application	`arn:${Partition}:servicecatalog:${Region}:${Account}:/applications/${ApplicationId}`	aws:ResourceTag/${TagKey}
Attribute Group	`arn:${Partition}:servicecatalog:${Region}:${Account}:/attribute-groups/${AttributeGroupId}`	aws:ResourceTag/${TagKey}
Portfolio	`arn:${Partition}:catalog:${Region}:${Account}:portfolio/${PortfolioId}`	aws:ResourceTag/${TagKey}
Product	`arn:${Partition}:catalog:${Region}:${Account}:product/${ProductId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Service Catalog

AWS Service Catalog definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

> **Note**
>
> Beispielrichtlinien, die zeigen, wie Sie diese Bedingungsschlüssel in IAM-Richtlinien verwenden können, finden Sie unter Beispiel-Zugriffsrichtlinien für bereitgestelltes Product Management im Administratorleitfaden von Service Catalog.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString
servicecatalog:Resource	Filtert den Zugriff, indem gesteuert wird, welcher Wert als Ressourcen-Parameter in einer AppRegistry-Associate-Resource-API angegeben werden kann	Zeichenfolge
servicecatalog:ResourceType	Filtert den Zugriff, indem gesteuert wird, welcher Wert als ResourceType-Parameter in einer AppRegistry-Associate-Resource-API angegeben werden kann	Zeichenfolge
servicecatalog:accountLevel	Filtert den Zugriff nach Benutzern, um Aktionen für Ressourcen anzuzeigen und auszuführen, die von beliebigen Benutzern im Konto erstellt wurden	Zeichenfolge
servicecatalog:roleLevel	Filtert den Zugriff nach Benutzern, um Aktionen für Ressourcen anzuzeigen und auszuführen, die entweder von ihnen oder von Personen erstellt wurden, die mit derselben Rolle verbunden sind	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
servicecatalog:userLevel	Filtert den Zugriff nach Benutzern, um Aktionen nur für Ressourcen anzuzeigen und auszuführen, die sie erstellt haben	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für AWS-Service, der verwaltete private Netzwerke bereitstellt

AWS-Service, der verwaltete private Netzwerke bereitstellt (Servicepräfix: `private-networks`), stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS-Service, der verwaltete private Netzwerke bereitstellt, definierte Aktionen
- Vom AWS-Service, der verwaltete private Netzwerke bereitstellt, definierte Ressourcentypen
- Bedingungsschlüssel für AWS-Service, der verwaltete private Netzwerke bereitstellt

Von AWS-Service, der verwaltete private Netzwerke bereitstellt, definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcknowledgeOrderReceipt	Gewährt die Berechtigung, den Eingang einer Bestellung zu bestätigen	Schreiben	order*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ActivateDeviceIdentifier	Gewährt die Berechtigung zum Aktivieren einer Gerätekennung	Schreiben	device-identifier*		
				aws:ResourceTag/${TagKey}	
ActivateNetworkSite	Gewährt die Berechtigung zum Aktivieren einer Netzwerkseite	Schreiben	network-site*		
			order*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ConfigureAccessPoint	Gewährt die Berechtigung zum Konfigurieren eines Zugangspunkts	Schreiben	network-resource*		
CreateNetwork	Gewährt die Berechtigung zum Erstellen eines Netzwerks	Schreiben	network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNetworkSite	Gewährt die Berechtigung zum Erstellen einer Netzwerkseite	Schreiben	network*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
DeactivateDeviceIdentifier	Gewährt die Berechtigung zum Deaktivieren einer Gerätekennung	Schreiben	device-identifier*		
DeleteNetwork	Gewährt die Berechtigung zum Löschen eines Netzwerks	Schreiben	network*		
DeleteNetworkSite	Gewährt die Berechtigung zum Löschen einer Netzwerkseite	Schreiben	network-site*		
GetDeviceIdentifier	Gewährt die Berechtigung zum Abrufen einer Gerätekennung	Lesen	device-identifier*		
				aws:ResourceTag/${TagKey}	
GetNetwork	Gewährt die Berechtigung zum Abrufen eines Netzwerks	Lesen	network*		
				aws:ResourceTag/${TagKey}	
GetNetworkResource	Gewährt die Berechtigung zum Abrufen einer Netzwerkressource	Lesen	network-resource*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
GetNetworkSite	Gewährt die Berechtigung zum Abrufen einer Netzwerksite	Lesen	network-site*		
				aws:ResourceTag/${TagKey}	
GetOrder	Gewährt die Berechtigung zum Abrufen eines Netzauftrags	Lesen	order*		
				aws:ResourceTag/${TagKey}	
ListDeviceIdentifiers	Gewährt die Berechtigung zum Auflisten von Geräteken nung	Auflisten	network*		
ListNetworkResources	Gewährt die Berechtigung zum Auflisten von Netzwerkressourcen	Auflisten	network*		
ListNetworkSites	Gewährt die Berechtigung zum Auflisten von Netzwerksiten	Auflisten	network*		
ListNetworks	Gewährt die Berechtigung zum Auflisten von Netzwerken	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListOrders	Gewährt die Berechtigung zum Auflisten von Netzaufträgen	Auflisten	network*		
ListTagsForResource	Gewährt Berechtigungen zum Zurückgeben einer Liste der Tags für eine Ressource	Auflisten			
Ping	Gewährt die Berechtigung zum Prüfen des Services	Lesen			
StartNetworkResourceUpdate	Gewährt die Berechtigung zum Starten einer Aktualisierung auf der angegebenen Netzwerkressource	Schreiben	network-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags der angegebenen Ressource	Markierung	device-identifier		
			network		
			network-resource		
			network-site		
			order		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus der angegebenen Ressource	Markierung	device-identifier		
			network		
			network-resource		
			network-site		
			order		
				aws:TagKeys	
UpdateNetworkSite	Gewährt die Berechtigung zum Aktualisieren einer Netzwerkseite	Schreiben	network-site*		
UpdateNetworkSitePlan	Gewährt die Berechtigung zum Aktualisieren eines Plans auf einer Netzwerkseite	Schreiben	network-site*		

Vom AWS-Service, der verwaltete private Netzwerke bereitstellt, definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
network	`arn:${Partition}:private-networks:${Region}:${Account}:network/${NetworkName}`	aws:ResourceTag/${TagKey}
network-site	`arn:${Partition}:private-networks:${Region}:${Account}:network-site/${NetworkName}/${NetworkSiteName}`	aws:ResourceTag/${TagKey}
network-resource	`arn:${Partition}:private-networks:${Region}:${Account}:network-resource/${NetworkName}/${ResourceId}`	aws:ResourceTag/${TagKey}
order	`arn:${Partition}:private-networks:${Region}:${Account}:order/${NetworkName}/${OrderId}`	aws:ResourceTag/${TagKey}
device-identifier	`arn:${Partition}:private-networks:${Region}:${Account}:device-identifier/${NetworkName}/${DeviceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS-Service, der verwaltete private Netzwerke bereitstellt

Der AWS-Service, der verwaltete private Netzwerke bereitstellt, definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können.

Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Prüfen des Vorhandenseins von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach der Prüfung von Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüsseln in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Service Quotas

Service Quotas (Servicepräfix: `servicequotas`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Service Quotas definierte Aktionen
- Von Service Quotas definierte Ressourcentypen
- Bedingungsschlüssel für -Service-Quotas

Von Service Quotas definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateServiceQuotaTemplate	Gewährt die Berechtigung zum Zuordnen der Service Quotas-Vorlage zu Ihrer Organisation.	Write			organizations:DescribeOrganization organizations:EnableAWSServiceAccess
DeleteServiceQuotaIncreaseRequestFromTemplate	Gewährt die Berechtigung zum Entfernen des angegebenen Servicekontingents aus der Service Quotas-Vorlage	Write			organizations:DescribeOrganization
DisassociateServiceQuotaTemplate	Gewährt die Berechtigung zum Trennen der Service Quotas-Vorlage von Ihrer Organisation.	Schreiben			organizations:DescribeOrganization
GetAWSDefaultServiceQuota	Erteilt die Erlaubnis, die Details für das angegebene Dienstkontingent, einschließlich des AWS Standardwerts, zurückzugeben	Lesen			
GetAssociationForServiceQuotaTemplate	Erteilt die Berechtigung zum Abrufen des ServiceQuotaTemplateAssociationStatus Werts, der Ihnen mitteilt, ob die Vorlage Service Quotas	Lesen			organizations:DescribeOrganization

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Servicekontingente einer Organisation zugeordnet ist				
GetRequestedServiceQuotaChange	Gewährt die Berechtigung zum Abrufen der Details für eine bestimmte Anforderung zum Anheben des Servicekontingents.	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetServiceQuota	Gewährt die Berechtigung zum Zurückgeben der Details für das angegebene Servicekontingent, einschließlich des angewendeten Werts.	Read			autoscaling:DescribeAccountLimits cloudformation:DescribeAccountLimits dynamodb:DescribeLimits elasticloadbalancing:DescribeAccountLimits iam:GetAccountSummary kinesis:DescribeLimits rds:DescribeAccountAttributes

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					route53:GetAccountLimit
GetServiceQuotaIncreaseRequestFromTemplate	Gewährt die Berechtigung zum Abrufen der Details für eine Anforderung zum Anheben des Servicekontingents aus der Service Quotas-Vorlage.	Lesen			organizations:DescribeOrganization
ListAWSDefaultServiceQuotas	Erteilt die Berechtigung, alle Standard-Servicekontingenten für den angegebenen AWS Dienst aufzulisten	Lesen			
ListRequestedServiceQuotaChangeHistory	Gewährt die Berechtigung zum Anfordern einer Liste der Änderungen an Kontingenten für einen Service.	Read			
ListRequestedServiceQuotaChangeHistoryByQuota	Gewährt die Berechtigung zum Anfordern einer Liste der Änderungen an bestimmten Service-Quotas.	Read			
ListServiceQuotaIncreaseRequestsInTemplate	Gewährt die Berechtigung zum Zurückgeben einer Liste der Servicekontingentanforderungen aus der Service Quotas-Vorlage.	Lesen			organizations:DescribeOrganization

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListServiceQuotas	Erteilt die Berechtigung, alle Dienstkontingente für den angegebenen AWS Dienst in diesem Konto in dieser Region aufzulisten	Lesen			autoscaling:DescribeAccountLimits cloudformation:DescribeAccountLimits dynamodb:DescribeLimits elasticloadbalancing:DescribeAccountLimits iam:GetAccountSummary kinesis:DescribeLimits rds:DescribeAccountAttributes

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					route53:GetAccountLimit
ListServices	Erteilt die Erlaubnis, die in Service Quotas verfügbaren AWS Dienste aufzulisten	Lesen			
ListTagsForResource	Gewährt die Berechtigung zum Anzeigen der Tags in einer SQ-Ressource	Lesen			
PutServiceQuotaIncreaseRequestIntoTemplate	Gewährt die Berechtigung zum Definieren und Hinzufügen einer Quote zur Service Quota-Vorlage.	Write	quota		organizations:DescribeOrganization
				servicequotas:service	
RequestServiceQuotaIncrease	Gewährt die Berechtigung zum Absenden der Anforderung zum Anheben eines Servicekontingents.	Write	quota		
				servicequotas:service	
TagResource	Gewährt die Berechtigung, einer SQ-Ressource einen Satz von Tags zuzuordnen	Markieren		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UntagResource	Gewährt die Berechtigung, einen Satz von Tags aus einer SQ-Ressource zu entfernen, wenn die zu entfernenden Tags mit einem Satz von kundenbereitgestellten Tag-Schlüsseln übereinstimmen	Markieren		aws:TagKeys	

Von Service Quotas definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
quota	`arn:${Partition}:servicequotas:${Region}:${Account}:${ServiceCode}/${QuotaCode}`	

Bedingungsschlüssel für -Service-Quotas

Service Quotas definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString
servicequotas:service	Filtert den Zugriff nach dem angegebenen AWS Dienst	String

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon SES

Amazon SES (Servicepräfix: `ses`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon SES definierte Aktionen
- Von Amazon SES definierte Ressourcentypen
- Bedingungsschlüssel für Amazon SES

Von Amazon SES definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CloneReceiptRuleSet	Gewährt die Berechtigung zum Erstellen eines Empfangsregelsatzes durch Klonen eines vorhandenen	Write		ses:ApiVersion	
CreateConfigurationSet	Gewährt die Berechtigung zum Erstellen eines neuen Konfigurationssatzes	Write		ses:ApiVersion	
CreateConfigurationSetEventDestination	Gewährt die Berechtigung zum Erstellen eines Konfigurationssatz-Ereignisziels	Write		ses:ApiVersion	
CreateConfigurationSetTrackingOptions	Gewährt die Berechtigung zum Erstellen einer Mapping zwischen einem Konfigurationssatz und einer benutzerdefinierten Domain für die Verfolgung von Öffnungs- und Klickereignissen	Write		ses:ApiVersion	
CreateCustomVerificationEmailTemplate	Gewährt die Berechtigung zum Erstellen einer neuen benutzerdefinierten Verifizierungs-E-Mail-Vorlage	Write		ses:ApiVersion	
CreateReceiptFilter	Gewährt die Berechtigung zum Erstellen eines neuen IP-Adressfilters	Write		ses:ApiVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateReceiptRule	Gewährt die Berechtigung zum Erstellen einer Empfangsregel	Write		ses:ApiVersion	
CreateReceiptRuleSet	Gewährt die Berechtigung zum Erstellen eines leeren Empfangsregelsatzes	Write		ses:ApiVersion	
CreateTemplate	Gewährt die Berechtigung zum Erstellen einer E-Mail-Vorlage	Write		ses:ApiVersion	
DeleteConfigurationSet	Gewährt die Berechtigung zum Löschen eines vorhandenen Konfigurationssatzes	Write		ses:ApiVersion	
DeleteConfigurationSetEventDestination	Gewährt die Berechtigung zum Löschen eines Ereignisziels	Write		ses:ApiVersion	
DeleteConfigurationSetTrackingOptions	Gewährt die Berechtigung zum Löschen einer Mapping zwischen einem Konfigurationssatz und einer benutzerdefinierten Domain für die Verfolgung von Öffnungs- und Klickereignissen	Write		ses:ApiVersion	
DeleteCustomVerificationEmailTemplate	Gewährt die Berechtigung zum Löschen einer vorhandenen benutzerdefinierten Verifizierungs-E-Mail-Vorlage	Write		ses:ApiVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteIdentity	Gewährt die Berechtigung zum Löschen der angegebenen Identität	Write		ses:ApiVersion	
DeleteIdentityPolicy	Gewährt die Berechtigung zum Löschen der angegebenen Sendegenehmigungsrichtlinie für die angegebene Identität (eine E-Mail-Adresse oder eine Domain)	Berechtigungsverwaltung		ses:ApiVersion	
DeleteReceiptFilter	Gewährt die Berechtigung zum Löschen des angegebenen IP-Adressfilters	Write		ses:ApiVersion	
DeleteReceiptRule	Gewährt die Berechtigung zum Löschen des angegebenen Empfangsregelsatzes	Write		ses:ApiVersion	
DeleteReceiptRuleSet	Gewährt die Berechtigung zum Löschen des angegebenen Empfagsregelsatzes und aller darin enthaltenen Zahlungsregeln	Write		ses:ApiVersion	
DeleteTemplate	Gewährt die Berechtigung zum Löschen einer E-Mail-Vorlage	Write		ses:ApiVersion	
DeleteVerifiedEmailAddress	Gewährt die Berechtigung zum Löschen der angegebenen E-Mail-Adresse aus der Liste der bestätigten Adressen	Write		ses:ApiVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeActiveReceiptRuleSet	Gewährt die Berechtigung zum Zurückgeben der Metadaten und Empfangsregeln für den derzeit aktiven Empfangsregelsatz	Read		ses:ApiVersion	
DescribeConfigurationSet	Gewährt die Berechtigung zum Zurückgeben der Details des angegebenen Konfigurationssatzes	Read		ses:ApiVersion	
DescribeReceiptRule	Gewährt die Berechtigung zum Zurückgeben der Details der angegebenen Empfangsregel	Read		ses:ApiVersion	
DescribeReceiptRuleSet	Gewährt die Berechtigung zur Rückgabe der Details des angegebenen Empfangsregelsatzes	Read		ses:ApiVersion	
GetAccountSendingEnabled	Gewährt die Berechtigung zum Zurückgeben des E-Mail-Sendestatus Ihres Kontos	Read		ses:ApiVersion	
GetCustomVerificationEmailTemplate	Gewährt die Berechtigung, die benutzerdefinierte E-Mail-Verifizierungsvorlage für den von Ihnen angegebenen Vorlagennamen zurückzugeben	Read		ses:ApiVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetIdentityDkimAttributes	Gewährt die Berechtigung zum Zurückgeben des aktuellen Status von Easy DKIM Signing für eine Entität	Read		ses:ApiVersion	
GetIdentityMailFromDomainAttributes	Gewährt die Berechtigung zum Zurückgeben der benutzerdefinierten MAIL FROM-Attribute für eine Liste von Identitäten (E-Mail-Adressen und/oder Domains)	Read		ses:ApiVersion	
GetIdentityNotificationAttributes	Gewährt die Berechtigung zum Zurückgeben einer Struktur, die die Identitätsbenachrichtigungsattribute beschreibt, für eine gegebenen Liste verifizierter Identitäten (E-Mail-Adressen und/oder Domains)	Read		ses:ApiVersion	
GetIdentityPolicies	Gewährt die Berechtigung, die angeforderten Sendeautorisierungsrichtlinien für die gegebene Identität (eine E-Mail-Adresse oder eine Domain) zurückzugeben	Read		ses:ApiVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetIdentityVerificationAttributes	Gewährt die Berechtigung zum Zurückgeben des Überprüfungsstatus und (für Domain-Identitäten) dds Überprüfungstokens für eine Liste von Identitäten	Read		ses:ApiVersion	
GetSendQuota	Gewährt die Berechtigung zum Zurückgeben des aktuellen Sendelimits des Benutzers	Read		ses:ApiVersion	
GetSendStatistics	Gewährt die Berechtigung zum Zurückgeben der sendenden Statistiken des Benutzers	Read		ses:ApiVersion	
GetTemplate	Gewährt die Berechtigung zum Zurückgeben des Vorlagenobjekts (enthält Betreff, HTML-Bestandteil und Textbestandteil) für die von Ihnen angegebene Vorlage	Read		ses:ApiVersion	
ListConfigurationSets	Gewährt die Berechtigung, alle Konfigurationssätze für Ihr Konto aufzulisten	List		ses:ApiVersion	
ListCustomVerificationEmailTemplates	Gewährt die Berechtigung, alle vorhandenen benutzerdefinierten Verifizierungs-E-Mail-Vorlagen für Ihr Konto aufzulisten	List		ses:ApiVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListIdentities	Gewährt die Berechtigung zum Auflisten der E-Mail-Identitäten für Ihr Konto	List		ses:ApiVersion	
ListIdentityPolicies	Gewährt die Berechtigung, alle E-Mail-Vorlagen für Ihr Konto aufzulisten	List		ses:ApiVersion	
ListReceiptFilters	Gewährt die Berechtigung zum Auflisten der mit Ihrem Konto verknüpften IP-Adressfilter	Read		ses:ApiVersion	
ListReceiptRuleSets	Gewährt die Berechtigung zum Auflisten der Empfangsregelsätze, die unter Ihrem Konto vorhanden sind	Read		ses:ApiVersion	
ListTemplates	Gewährt die Berechtigung zum Auflisten der in Ihrem Konto vorhandenen E-Mail-Vorlagen	List		ses:ApiVersion	
ListVerifiedEmailAddresses	Gewährt die Berechtigung zum Auflisten aller in Ihrem Konto verifizierter E-Mail-Adressen	Read		ses:ApiVersion	
PutConfigurationSetDeliveryOptions	Gewährt die Berechtigung zum Hinzufügen oder Aktualisieren der Bereitstellungsoptionen für einen Konfigurationssatz	Write		ses:ApiVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutIdentityPolicy	Gewährt die Berechtigung zum Hinzufügen oder Aktualisieren einer Sendegenehmigungsrichtlinie für die angegebene Identität (eine E-Mail-Adresse oder eine Domain)	Berechtigungsverwaltung		ses:ApiVersion	
ReorderReceiptRuleSet	Gewährt die Berechtigung zur Neusortierung der Wareneingangsregeln innerhalb eines Empfangsregelsatzes	Write		ses:ApiVersion	
SendBounce	Gewährt die Berechtigung zum Generieren einer Bounce-Nachricht und Senden an den Sender einer E-Mail, die Sie über Amazon SES erhalten haben	Write	identity*		
				ses:ApiVersion ses:FromAddress	
SendBulkTemplatedEmail	Gewährt die Berechtigung, eine E-Mail-Nachricht für mehrere Ziele zu verfassen	Write	identity*		
			template*		
			configuration-set		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SendCustomVerificationEmail	Gewährt die Berechtigung zum Hinzufügen einer E-Mail-Adresse zur Liste der Identitäten und versucht, diese zu überprüfen	Write	identity*		
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SendEmail	Gewährt die Berechtigung zum Senden einer E-Mail	Write	identity*		
			configuration-set		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SendRawEmail	Gewährt die Berechtigung zum Senden einer E-Mail-Nachricht mit dem vom Kunden angegebenen Header und Inhalt	Write	identity* configuration-set		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SendTemplatedEmail	Gewährt die Berechtigung zum Verfassen einer E-Mail-Nachricht mit einer E-Mail-Vorlage	Write	identity* template* configuration-set		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SetActiveReceiptRuleSet	Gewährt die Berechtigung zum Festlegen des angegebenen Empfangsregelsatzes als aktiven Empfangsregelsatz	Write		ses:ApiVersion	
SetIdentityDkimEnabled	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren der einfachen DKIM-Signierung von E-Mails, die von einer Identität gesendet wurden	Write		ses:ApiVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SetIdentityFeedbackForwardingEnabled	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren, ob Amazon SES Bounce- und Beschwerdebenachrichtigungen für eine Identität (eine E-Mail-Adresse oder eine Domain) weiterleitet	Write		ses:ApiVersion	
SetIdentityHeadersInNotificationsEnabled	Gewährt die Berechtigung zum Festlegen für eine gegebene Identität (E-Mail-Adresse oder Domain), ob Amazon SES die ursprünglichen E-Mail-Header in die Amazon Simple Notification Service (Amazon SNS)-Benachrichtigungen eines angegebenen Typs einschließt	Write		ses:ApiVersion	
SetIdentityMailFromDomain	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren des benutzerdefinierten MAIL FROM-Domain-Setups für eine verifizierte Identität	Write		ses:ApiVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SetIdentityNotificationTopic	Gewährt die Berechtigung zum Festlegen eines Amazon Simple Notification Service (Amazon SNS)-Themas, das bei der Übermittlung von Benachrichtigungen für eine verifizierte Identität verwendet werden soll	Write		ses:ApiVersion	
SetReceiptRulePosition	Gewährt die Berechtigung zum Festlegen der Position der angegebenen Empfangsregel im Empfangsregelsatz	Write		ses:ApiVersion	
TestRenderTemplate	Gewährt die Berechtigung zum Erstellen einer Vorschau des MIME-Inhalts einer E-Mail, wenn eine Vorlage und ein Satz von Ersatzdaten übergeben werden	Write		ses:ApiVersion	
UpdateAccountSendingEnabled	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren des E-Mail-Versands für Ihr Konto	Write		ses:ApiVersion	
UpdateConfigurationSetEventDestination	Gewährt die Berechtigung zum Aktualisieren des Ereignisziels eines Konfigurationssatzes	Write		ses:ApiVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateConfigurationSetReputationMetricsEnabled	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren der Veröffentlichung von Reputationsmetriken für E-Mails, die mit einem bestimmten Konfigurationssatz gesendet werden	Write		ses:ApiVersion	
UpdateConfigurationSetSendingEnabled	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren des E-Mail-Versands für Nachrichten, die mit einem bestimmten Konfigurationssatz gesendet werden	Write		ses:ApiVersion	
UpdateConfigurationSetTrackingOptions	Gewährt die Berechtigung zum Ändern einer Mapping zwischen einem Konfigurationssatz und einer benutzerdefinierten Domain für die Verfolgung von Öffnungs- und Klickereignissen	Write		ses:ApiVersion	
UpdateCustomVerificationEmailTemplate	Gewährt die Berechtigung zum Aktualisieren einer vorhandenen benutzerdefinierten Verifizierungs-E-Mail-Vorlage	Write		ses:ApiVersion	
UpdateReceiptRule	Gewährt die Berechtigung zum Aktualisieren einer Empfangsregel	Write		ses:ApiVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateTemplate	Gewährt die Berechtigung zum Aktualisieren einer E-Mail-Vorlage	Write		ses:ApiVersion	
VerifyDomainDkim	Gewährt die Berechtigung zum Zurückgeben eines Satzes DKIM-Tokens für eine Domain	Schreiben		ses:ApiVersion	
VerifyDomainIdentity	Gewährt die Berechtigung zum Verifizieren einer Domain	Schreiben		ses:ApiVersion	
VerifyEmailAddress	Gewährt die Berechtigung zum Verifizieren einer E-Mail-Adresse	Schreiben		ses:ApiVersion	
VerifyEmailIdentity	Gewährt die Berechtigung zum Verifizieren einer E-Mail-Identität	Schreiben		ses:ApiVersion	

Von Amazon SES definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
configuration-set	`arn:${Partition}:ses:${Region}:${Account}:configuration-set/${ConfigurationSetName}`	
custom-verification-email-template	`arn:${Partition}:ses:${Region}:${Account}:custom-verification-email-template/${TemplateName}`	
identity	`arn:${Partition}:ses:${Region}:${Account}:identity/${IdentityName}`	
template	`arn:${Partition}:ses:${Region}:${Account}:template/${TemplateName}`	

Bedingungsschlüssel für Amazon SES

Amazon SES definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
ses:ApiVersion	Filtert Aktionen basierend auf der SES-API-Version.	Zeichenfolge
ses:FeedbackAddress	Filtert Aktionen basierend auf der „Return-Path“-Adresse, die festlegt, wohin Unzustellbarkeitsnachrichten und Beschwerden von der Funktion für E-Mail-Feedback-Weiterleitung gesendet werden	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
ses:FromAddress	Filtert Aktionen basierend auf der „Von“-Adresse einer Nachricht	Zeichenfolge
ses:FromDisplayName	Filtert Aktionen basierend auf der „Von“-Adresse, die als Anzeigename einer Nachricht verwendet wird	Zeichenfolge
ses:Recipients	Filtert Aktionen basierend auf den Empfängeradressen einer Nachricht, einschließlich der „An“-, „CC“- und „BCC“-Adressen	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Shield

AWS Shield (Servicepräfix: `shield`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Shield definierte Aktionen
- Von AWS Shield definierte Ressourcentypen
- Bedingungsschlüssel für AWS Shield

Von AWS Shield definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Associate DRTLogBucket	Gewährt die Berechtigung zum Autorisieren des DDoS Response Teams für den Zugriff auf den angegebenen Amazon-S3-Bucket mit Ihren Ablauf-Protokollen	Write			s3:GetBucketPolicy s3:PutBucketPolicy
Associate DRTRole	Gewährt die Berechtigung zum Autorisieren des DDoS Response Teams mithilfe der angegebenen Rolle für den Zugriff auf Ihr AWS-Konto zur Unterstützung der DDoS-Angriffsminimierung bei potenziellen Angriffen.	Write			iam:GetRole iam:ListAttachedRolePolicies iam:PassRole
Associate HealthCheck	Gewährt die Berechtigung zum Hinzufügen einer gesundheitsbasierten Erkennung zum Shield Advanced-Schutz für eine Ressource	Write	protection*		route53:GetHealthCheck
				aws:ResourceTag/${TagKey}	
Associate ProactiveEngagementDetails	Gewährt die Berechtigung zum Initialisieren eines proaktiven Engagements und zum Festlegen der Liste der Kontakte, die das DDoS Response Team (DRT) verwenden soll	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateProtection	Gewährt die Berechtigung zum Aktivieren des DDoS-Schutzservices für einen bestimmten Ressourcen-ARN	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProtectionGroup	Gewährt die Berechtigung zum Erstellen einer Gruppierung geschützter Ressourcen, damit sie als Kollektiv behandelt werden können	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscription	Gewährt die Berechtigung zum Aktivieren des Abonnements	Write			
DeleteProtection	Gewährt die Berechtigung zum Löschen eines bestehenden Schutzes	Write	protection*		
				aws:ResourceTag/${TagKey}	
DeleteProtectionGroup	Gewährt die Berechtigung zum Entfernen der angegebenen Schutzgruppe	Write	protection-group*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteSubscription	Gewährt die Berechtigung zum Deaktivieren des Abonnements	Write			
DescribeAttack	Gewährt die Berechtigung zum Abrufen von Angriffsdetails	Read	attack*		
DescribeAttackStatistics	Gewährt die Berechtigung zum Beschreiben von Informationen über die Anzahl und Art der Angriffe, die AWS Shield im letzten Jahr entdeckt hat.	Read			
DescribeDRTAccess	Gewährt die Berechtigung zum Zurückgeben der aktuellen Rolle und der Liste der Amazon S3-Protokoll-Buckets, die vom DDoS Response Team für den Zugriff auf Ihr AWS-Konto zur Unterstützung der Angriffsminimierung verwendet werden.	Read			
DescribeEmergencyContactSettings	Gewährt die Berechtigung zum Auflisten der E-Mail-Adressen, über die das DRT sich bei einem mutmaßlichen Angriff mit Ihnen in Verbindung setzen kann.	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeProtection	Gewährt die Berechtigung zum Abrufen von Schutzinformationen	Read	protection*		
				aws:ResourceTag/${TagKey}	
DescribeProtectionGroup	Gewährt die Berechtigung zum Beschreiben der Spezifikation für die angegebene Schutzgruppe	Read	protection-group*		
				aws:ResourceTag/${TagKey}	
DescribeSubscription	Gewährt die Berechtigung zum Abrufen von Abonnementdetails wie Startzeit	Lesen			
DisableApplicationLayerAutomaticResponse	Gewährt die Berechtigung zum Deaktivieren der automatischen Reaktion der Anwendungsschicht für Shield-Advanced-Schutz für eine Ressource	Schreiben			
DisableProactiveEngagement	Gewährt die Berechtigung zum Entfernen der Autorisierung des DDoS Response Teams (DRT), um Kontakte über Eskalationen zu benachrichtigen	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateDRTLogBucket	Gewährt die Berechtigung zum Aufheben des Zugriffs des DDoS Response Teams auf den angegebenen Amazon-S3-Bucket, der Ihre Ablauf-Protokolle enthält.	Write			s3:DeleteBucketPolicy s3:GetBucketPolicy s3:PutBucketPolicy
DisassociateDRTRole	Gewährt die Berechtigung zum Entfernen des Zugriffs des DDoS Response-Teams auf Ihr AWS-Konto.	Write			
DisassociateHealthCheck	Gewährt die Berechtigung zum Entfernen der gesundheitsbasierten Erkennung aus dem Shield Advanced-Schutz für eine Ressource	Schreiben	protection*		
				aws:ResourceTag/${TagKey}	
EnableApplicationLayerAutomaticResponse	Gewährt die Berechtigung zum Aktivieren der automatischen Reaktion der Anwendungsschicht für Shield-Advanced-Schutz für eine Ressource	Schreiben			cloudfront:GetDistribution iam:CreateServiceLinkedRole iam:GetRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
EnableProactiveEngagement	Gewährt die Berechtigung zum Autorisieren des DDoS Response Teams (DRT), E-Mail und Telefon zu verwenden, um Kontakte über Eskalationen zu benachrichtigen	Write			
GetSubscriptionState	Gewährt die Berechtigung zum Abrufen des Status eines Abonnements	Read			
ListAttacks	Gewährt die Berechtigung zum Auflisten aller bestehenden Angriffe	List			
ListProtectionGroups	Gewährt die Berechtigung zum Abrufen der Schutzgruppen für das Konto	List			
ListProtections	Gewährt die Berechtigung zum Auflisten aller bestehenden Schutzmaßnahmen	List			
ListResourcesInProtectionGroup	Gewährt die Berechtigung zum Abrufen der Ressourcen, die in der Schutzgruppe enthalten sind	List	protection-group*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Abrufen von Informationen über AWS-Tags für einen bestimmten Amazon-Ressourcennamen (ARN) in AWS Shield.	Read	protection		
			protection-group		
TagResource	Gewährt die Berechtigung zum Hinzufügen oder Aktualisieren von Tags für eine Ressource in AWS Shield.	Markieren	protection		
			protection-group		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Ressource in AWS Shield.	Markierung	protection		
			protection-group		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateApplicationLayerAutomaticResponse	Gewährt die Berechtigung zum Aktualisieren der automatischen Reaktion der Anwendungsschicht für Shield-Advanced-Schutz für eine Ressource	Schreiben			
UpdateEmergencyContactSettings	Gewährt die Berechtigung zum Aktualisieren der Details der Liste mit E-Mail-Adressen, über die das DRT sich bei einem mutmaßlichen Angriff mit Ihnen in Verbindung setzen kann.	Write			
UpdateProtectionGroup	Gewährt die Berechtigung zum Aktualisieren einer bestehenden Schutzgruppe	Write	protection-group*		
				aws:ResourceTag/${TagKey}	
UpdateSubscription	Gewährt die Berechtigung zum Aktualisieren der Details eines bestehenden Abonnements	Write			

Von AWS Shield definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden

können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
attack	`arn:${Partition}:shield::${Account}:attack/${Id}`	
protection	`arn:${Partition}:shield::${Account}:protection/${Id}`	aws:ResourceTag/${TagKey}
protection-group	`arn:${Partition}:shield::${Account}:protection-group/${Id}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Shield

AWS Shield definiert die folgenden Bedingungsschlüssel, die in einem `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung.	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf den Tag-Schlüssel-Wert-Paaren, die an die Ressource angefügt wurden.	Zeichenfolge
aws:TagKeys	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Signer

AWS Signer (Servicepräfix: `signer`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Signer definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddProfilePermission	Gewährt die Berechtigung zum Hinzufügen kontoüber greifender Berechtigungen zu einem Signierungsprofil	Berechtigungsverwaltung	signing-profile*		
CancelSigningProfile	Gewährt die Berechtigung, den Status eines Signierungsprofils zu CANCELED zu ändern	Write	signing-profile*		
				signer:ProfileVersion	
DescribeSigningJob	Gewährt die Berechtigung zum Abrufen von Informati	Lesen	signing-job*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	onen zu einer bestimmten Signierungsaufgabe				
GetRevocationStatus	Gewährt die Berechtigung zum Abfragen von Widerrufsinformationen zu Signaturressourcen	Lesen	signing-job*		
			signing-profile*		
GetSigningPlatform	Gewährt die Berechtigung zum Abrufen von Informationen zu einer bestimmten Signierungsplattform	Read			
GetSigningProfile	Gewährt die Berechtigung zum Abrufen von Informationen zu einem bestimmten Signierungsprofil	Read	signing-profile*		
				signer:ProfileVersion	
ListProfilePermissions	Gewährt die Berechtigung, die einem Signierungsprofil zugeordneten kontoüber greifenden Berechtigungen aufzulisten	Read	signing-profile*		
ListSigningJobs	Gewährt die Berechtigung zum Auflisten aller Signierungsaufgaben in Ihrem Konto	List			
ListSigningPlatforms	Gewährt die Berechtigung zum Auflisten aller verfügbaren Signierungsplattformen	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListSigningProfiles	Gewährt die Berechtigung zum Auflisten aller Signierungsprofile in Ihrem Konto	List			
ListTagsForResource	Gewährt die Berechtigung, die einem Signierungsprofil zugeordneten Tags aufzulisten	Read	signing-profile*		
PutSigningProfile	Gewährt die Berechtigung zum Erstellen eines neuen Signierungsprofils	Write		aws:RequestTag/${TagKey} aws:TagKeys	
RemoveProfilePermission	Gewährt die Berechtigung zum Entfernen kontoüber greifender Berechtigungen aus einem Signierungsprofil	Berechtigungsverwaltung	signing-profile*		
RevokeSignature	Gewährt die Berechtigung, den Status einer Signierungsaufgabe zu REVOKED zu ändern	Write	signing-job*		
				signer:ProfileVersion	
RevokeSigningProfile	Gewährt die Berechtigung, den Status eines Signierungsprofils zu REVOKED zu ändern	Schreiben	signing-profile*		
				signer:ProfileVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SignPayload	Gewährt die Berechtigung, einen Signierungsauftrag für die bereitgestellte Nutzlast zu initiieren	Schreiben	signing-profile*		
				signer:ProfileVersion	
StartSigningJob	Gewährt die Berechtigung, eine Signierungsaufgabe für den bereitgestellten Code zu initiieren	Write	signing-profile*		
				signer:ProfileVersion	
TagResource	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Tags zu einem Signierungsprofil	Markieren	signing-profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung, ein oder mehrere Tags aus einem Signierungsprofil zu entfernen	Markieren	signing-profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Von AWS Signer definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
signing-profile	`arn:${Partition}:signer:${Region}:${Account}:/signing-profiles/${ProfileName}`	aws:ResourceTag/${TagKey}
signing-job	`arn:${Partition}:signer:${Region}:${Account}:/signing-jobs/${JobId}`	

Bedingungsschlüssel für AWS Signer

AWS Signer definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den zulässigen Werten für jedes der Tags	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Tag-Wert, der der Ressource zugeordnet ist	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach dem Vorhandensein verbindlicher Tags in der Anforderung	ArrayOfString
signer:ProfileVersion	Filtert den Zugriff nach der Version des Signierungsprofils	Zeichenfolge

Aktionen, Ressourcen und Bedingungstasten für AWS Signin

AWS Signin (Dienstpräfix:`signin`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Signin definierte Aktionen AWS
- Von AWS Signin definierte Ressourcentypen
- Bedingungsschlüssel für Signin AWS

Von Signin definierte Aktionen AWS

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTrustedIdentityPropagationApplicationForConsole	Erteilt die Berechtigung zum Erstellen einer Identity Center-Anwendung, die die Instanz der Organisation AWS Management Console auf einem Identity Center darstellt	Schreiben			sso:CreateApplication sso:GetSharedSsoConfiguration sso:ListApplications sso:PutApplicationAccessScope sso:PutApplicationAssignmentConfiguration sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTrustedIdentityPropagationApplicationsForConsole	Erteilt die Berechtigung, alle Identity Center-Anwendungen aufzulisten, die Folgendes repräsentieren AWS Management Console	Auflisten			sso:GetSharedSsoConfiguration sso:ListApplications

Von AWS Signin definierte Ressourcentypen

AWS Signin unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource` Element einer IAM-Richtlinienanweisung. Um den Zugriff auf AWS Signin zu ermöglichen, geben Sie dies in Ihrer Richtlinie an`"Resource": "*"`.

Bedingungsschlüssel für Signin AWS

Signin hat keine dienstspezifischen Kontextschlüssel, die in Richtlinienerklärungen verwendet werden können. `Condition` Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Simple Email Service v2

Amazon Simple Email Service v2 (Servicepräfix: `ses`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.

- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Simple Email Service v2 definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetMetricData	Gewährt die Berechtigung zum Abrufen von Metriken für Ihre Aktivität	Lesen	configuration-set		
			identity		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CancelExportJob	Gewährt die Berechtigung zum Abbrechen eines Exportauftrags	Schreiben	export-job*		
				ses:ApiVersion ses:ExportSourceType	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateConfigurationSet	Gewährt die Berechtigung zum Erstellen eines neuen Konfigurationssatzes	Schreiben	configuration-set*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateConfigurationSetEventDestination	Gewährt die Berechtigung zum Erstellen eines Konfigurationssatz-Ereignisziels	Schreiben	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CreateContact	Gewährt die Berechtigung zum Erstellen eines Kontakts	Schreiben	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateContactList	Gewährt die Berechtigung zum Erstellen einer Kontaktliste	Schreiben	contact-list*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateCustomVerificationEmailTemplate	Gewährt die Berechtigung zum Erstellen einer neuen benutzerdefinierten Verifizierungs-E-Mail-Vorlage	Schreiben	custom-verification-email-template*		
				ses:ApiVersion	
CreateDedicatedIpPool	Gewährt die Berechtigung zum Erstellen eines neuen Pools dedizierter IP-Adressen	Schreiben	dedicated-ip-pool*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDeliverabilityTestReport	Gewährt die Berechtigung zum Erstellen eines neuen prädiktiven Posteingangs-Platzierungstests	Schreiben	identity*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateEmailIdentity	Gewährt die Berechtigung, den Prozess der Überprüfung einer E-Mail-Identität zu starten	Schreiben	identity*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateEmailIdentityPolicy	Gewährt die Berechtigung zum Erstellen der angegebenen Sendegenehmigungsrichtlinie für die angegebene Identität	Berechtigungsverwaltung	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CreateEmailTemplate		Schreiben	template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Gewährt die Berechtigung zum Erstellen einer E-Mail-Vorlage			ses:ApiVersion	
CreateExportJob	Gewährt die Berechtigung zum Erstellen eines Exportauftrags	Schreiben		ses:ApiVersion ses:ExportSourceType	
CreateImportJob	Gewährt die Berechtigung zum Erstellen einer Importaufgabe für ein Datenziel	Schreiben		ses:ApiVersion	
DeleteConfigurationSet	Gewährt die Berechtigung zum Löschen eines vorhandenen Konfigurationssatzes	Schreiben	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteConfigurationSetEventDestination	Gewährt die Berechtigung zum Löschen eines Ereignisziels	Schreiben	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteContact	Gewährt die Berechtigung, einen Kontakt aus einer Kontaktliste zu löschen	Schreiben	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteContactList	Gewährt die Berechtigung, eine Kontaktliste mit allen ihren Kontakten zu löschen	Schreiben	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteCustomVerificationEmailTemplate	Gewährt die Berechtigung zum Löschen einer vorhandenen benutzerdefinierten Verifizierungs-E-Mail-Vorlage	Schreiben	custom-verification-email-template*		
				ses:ApiVersion	
DeleteDedicatedIpPool	Gewährt die Berechtigung zum Löschen eines dedizierten IP-Pools	Schreiben	dedicated-ip-pool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteEmailIdentity	Gewährt die Berechtigung zum Löschen einer E-Mail-Identität	Schreiben	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteEmailIdentityPolicy	Gewährt die Berechtigung zum Löschen der angegebenen Sendegenehmigungsrichtlinie für die angegebene Identität (eine E-Mail-Adresse oder eine Domain)	Berechtigungsverwaltung	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteEmailTemplate	Gewährt die Berechtigung zum Löschen einer E-Mail-Vorlage	Schreiben	template*		
				ses:ApiVersion	
DeleteSuppressedDestination	Gewährt die Berechtigung, eine E-Mail-Adresse aus der Unterdrückungsliste für Ihr Konto zu entfernen	Schreiben		ses:ApiVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAccount	Gewährt die Berechtigung, Informationen über den Status des E-Mail-Versands und die Funktionen Ihres Kontos zu erhalten	Lesen		ses:ApiVersion	
GetBlacklistReports	Gewährt die Berechtigung zum Abrufen einer Liste der Ablehnungslisten, auf denen Ihre dedizierten IP-Adressen oder nachverfolgten Domains angezeigt werden	Lesen		ses:ApiVersion	
GetConfigurationSet	Gewährt die Berechtigung zum Abrufen von Informationen über einen vorhandenen Konfigurationssatz	Lesen	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetConfigurationSetEventDestinations	Gewährt die Berechtigung zum Abrufen einer Liste von Ereigniszielen, die mit einem Konfigurationssatz verknüpft sind	Lesen	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetContact	Gewährt die Erlaubnis, einen Kontakt aus einer Kontaktliste zurückzugeben	Lesen	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetContactList	Gewährt die Erlaubnis, Metadaten der Kontaktliste zurückzugeben	Lesen	contact-list*		
				ses:ApiVersion	
GetCustomVerificationEmailTemplate	Gewährt die Berechtigung, die benutzerdefinierte E-Mail-Verifizierungsvorlage für den von Ihnen angegebenen Vorlagennamen zurückzugeben	Lesen	custom-verification-email-template*		
				ses:ApiVersion	
GetDedicatedIp	Gewährt die Berechtigung, Informationen über eine dedizierte IP-Adresse zu erhalten	Lesen		ses:ApiVersion	
GetDedicatedIpPool	Gewährt die Berechtigung, Informationen über einen dedizierten IP-Pool abzurufen	Lesen	dedicated-ip-pool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDedicatedIps	Gewährt die Berechtigung zum Auflisten der dedizierten IP-Adressen eines dedizierten IP-Pools	Lesen	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDeliverabilityDashboardOptions	Gewährt die Berechtigung zum Abrufen des Status des Zustellbarkeits-Dashboards	Lesen		ses:ApiVersion	
GetDeliverabilityTestReport	Gewährt die Berechtigung zum Abrufen der Ergebnisse eines prädiktiven Tests zur Platzierung im Posteingang	Lesen	deliverability-test-report*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetDomainDeliverabilityCampaign	Gewährt die Erlaubnis zum Abrufen aller Zustellbarkeitsdaten für eine bestimmte Kampagne	Lesen		ses:ApiVersion	
GetDomainStatisticsReport	Gewährt die Berechtigung zum Abrufen der Posteingangsplatzierungs- und Interaktionsraten für die Domains, die Sie zum Senden von E-Mails verwenden	Lesen	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetEmailIdentity	Gewährt die Berechtigung zum Abrufen von Informationen zu einer bestimmten Identität	Lesen	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetEmailIdentityPolicies	Gewährt die Berechtigung, die angeforderten Sendeautorisierungsrichtlinien für die gegebene Identität (eine E-Mail-Adresse oder eine Domain) zurückzugeben	Lesen	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetEmailTemplate	Gewährt die Berechtigung, das Vorlagenobjekt (enthält Betreff, HTML-Bestandteil und Textbestandteil) für die von Ihnen angegebene Vorlage zurückzugeben	Lesen	template*		
				ses:ApiVersion	
GetExportJob	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Exportauftrag	Lesen	export-job*		
				ses:ApiVersion ses:ExportSourceType	
GetImportJob	Gewährt die Berechtigung, Informationen über eine Importaufgabe bereitzustellen	Lesen	import-job*		
				ses:ApiVersion	
GetMessageInsights	Gewährt die Berechtigung zum Bereitstellen von Einblicken für eine Nachricht	Lesen		ses:ApiVersion	
GetSuppressedDestination	Gewährt die Berechtigung zum Abrufen von Informationen zu einer bestimmten E-Mail-Adresse, die auf der Unterdrückungsliste für Ihr Konto aufgeführt ist	Lesen		ses:ApiVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListConfigurationSets	Gewährt die Berechtigung, alle Konfigurationssätze für Ihr Konto aufzulisten	Auflisten		ses:ApiVersion	
ListContactLists	Gewährt die Berechtigung, alle für Ihr Konto verfügbaren Kontaktlisten aufzulisten	Auflisten		ses:ApiVersion	
ListContacts	Gewährt die Berechtigung, die in einer bestimmten Kontaktliste vorhandenen Kontakte aufzulisten	Auflisten	contact-list*		
				ses:ApiVersion	
ListCustomVerificationEmailTemplates	Gewährt die Berechtigung, alle vorhandenen benutzerdefinierten Verifizierungs-E-Mail-Vorlagen für Ihr Konto aufzulisten	Auflisten		ses:ApiVersion	
ListDedicatedIpPools	Gewährt die Berechtigung, alle dedizierten IP-Pools für Ihr Konto aufzulisten	Auflisten		ses:ApiVersion	
ListDeliverabilityTestReports	Gewährt die Berechtigung zum Abrufen der Liste der von Ihnen für Ihr Konto durchgeführten prädiktiven Tests zur Platzierung im Posteingang unabhängig von deren Status	Auflisten		ses:ApiVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDomainDeliverabilityCampaigns	Gewährt die Berechtigung zum Auflisten von Zustellbarkeitsdaten für Kampagnen, die eine bestimmte Domain zum Senden von E-Mails während eines bestimmten Zeitraums verwendet haben	Lesen		ses:ApiVersion	
ListEmailIdentities	Gewährt die Berechtigung zum Auflisten der E-Mail-Identitäten für Ihr Konto	Auflisten		ses:ApiVersion	
ListEmailTemplates	Gewährt die Berechtigung, alle E-Mail-Vorlagen für Ihr Konto aufzulisten	Auflisten		ses:ApiVersion	
ListExportJobs	Gewährt die Berechtigung, alle Exportaufträge für Ihr Konto aufzulisten	Auflisten		ses:ApiVersion ses:ExportSourceType	
ListImportJobs	Gewährt die Berechtigung, alle Importaufträge für Ihr Konto aufzulisten	Auflisten		ses:ApiVersion	
ListRecommendations	Gewährt die Berechtigung zum Auflisten von Empfehlungen für Ihr Konto	Lesen	identity		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListSuppressedDestinations	Gewährt die Berechtigung zum Auflisten von E-Mail-Adressen, die in der Unterdrückungsliste für Ihr Konto enthalten sind	Lesen		ses:ApiVersion	
ListTagsForResource	Gewährt die Berechtigung zum Aufrufen einer Liste der Tags (Schlüssel und Werte), die einer bestimmten Ressource für Ihr Konto zugeordnet sind	Lesen	configuration-set		
			contact-list		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		
				ses:ApiVersion	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutAccountDedicatedIpWarmupAttributes	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren des automatischen Aufwärmfeatures für dedizierte IP-Adressen	Schreiben		ses:ApiVersion	
PutAccountDetails	Gewährt die Berechtigung, Ihre Kontodaten zu aktualisieren	Schreiben		ses:ApiVersion	
PutAccountSendingAttributes	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren der Fähigkeit E-Mails für Ihr Konto zu senden	Schreiben		ses:ApiVersion	
PutAccountSuppressionAttributes	Gewährt die Berechtigung zum Ändern der Einstellungen für die Unterdrückungsliste auf Kontoebene	Schreiben		ses:ApiVersion	
PutAccountVdmAttributes	Gewährt die Berechtigung zum Ändern der Einstellungen für VDM für Ihr Konto	Schreiben		ses:ApiVersion	
PutConfigurationSetDeliveryOptions	Gewährt die Berechtigung zum Verknüpfen eines Konfigurationssatzes mit einem dedizierten IP-Pool	Schreiben	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutConfigurationSetReputationOptions	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren der Sammlung von Zuverlässigkeitsmetriken für E-Mails, die unter Verwendung eines bestimmten Konfigurationssatzes versendet werden	Schreiben	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetSendingOptions	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren des E-Mail-Versands für Nachrichten, die einen bestimmten Konfigurationssatz verwenden	Schreiben	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetSuppressionOptions	Gewährt die Berechtigung zum Angeben der Einstellungen für die Kontenunterdrückungsliste für einen bestimmten Konfigurationssatz	Schreiben	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutConfigurationSetTrackingOptions	Gewährt die Berechtigung zum Angeben einer benutzerdefinierten Domain, die für offene und Klicknachverfolgungs-Elemente in E-Mails verwendet werden soll, die Sie für einen bestimmten Konfigurationssatz versenden	Schreiben	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetVdmOptions	Gewährt die Berechtigung zum Überschreiben von VDM-Einstellungen auf Kontoebene für einen bestimmten Konfigurationssatz	Schreiben	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpInPool	Gewährt die Berechtigung zum Verschieben einer dedizierten IP-Adresse in einen bestehenden dedizierten IP-Pool	Schreiben	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpPoolScalingAttributes	Gewährt die Berechtigung zum Wechseln eines dedizierten IP-Pools von Standard auf Managed	Schreiben	dedicated-ip-pool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpWarmupAttributes	Gewährt die Berechtigung zum Festlegen dedizierter IP-Aufwärmattribute	Schreiben		ses:ApiVersion	
PutDeliverabilityDashboardOption	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren des Zustellbarkeits-Dashboards	Schreiben		ses:ApiVersion	
PutEmailIdentityConfigurationSetAttributes	Gewährt die Berechtigung zum Verknüpfen eines Konfigurationssatzes mit einer E-Mail-Identität	Schreiben	identity*		
			configuration-set		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutEmailIdentityDkimAttributes	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren der DKIM-Authentifizierung für eine E-Mail-Identität	Schreiben	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityDkimSigningAttributes	Gewährt die Berechtigung zum Konfigurieren oder Ändern der DKIM-Authentifizierungseinstellungen für eine E-Mail-Domain-Identität	Schreiben	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityFeedbackAttributes	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren der Feedback-Weiterleitung für eine E-Mail-Identität	Schreiben	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityMailFromAttributes	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren der benutzerdefinierten „Mail-From“-Domain-Konfiguration für eine E-Mail-Identität	Schreiben	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutSuppressedDestination	Gewährt die Berechtigung zum Hinzufügen einer E-Mail-Adresse zur Unterdrückungsliste	Schreiben		ses:ApiVersion	
SendBulkEmail	Gewährt die Berechtigung, eine E-Mail-Nachricht für mehrere Ziele zu verfassen	Schreiben	identity*		
			template*		
			configuration-set		
				ses:ApiVersion	
SendCustomVerificationEmail	Gewährt die Berechtigung, eine E-Mail-Adresse zur Liste der Identitäten hinzuzufügen und versucht, diese zu überprüfen	Schreiben	custom-verification-email-template*		
				ses:ApiVersion	
SendEmail	Gewährt die Berechtigung zum Senden einer E-Mail	Schreiben	identity*		
			configuration-set		
			template		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
TagResource	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Tags (Schlüssel und Werte) zu einer bestimmten Ressource	Markierung	configuration-set		
			contact-list		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
TestRenderEmailTemplate	Gewährt die Berechtigung zum Erstellen einer Vorschau des MIME-Inhalts einer E-Mail, wenn eine Vorlage und ein Satz von Ersatzdaten übergeben werden	Schreiben	template*		
				ses:ApiVersion	
UntagResource	Gewährt die Berechtigung zum Entfernen eines oder mehrerer Tags (Schlüssel und Werte) von einer bestimmten Ressource	Markierung	configuration-set		
			contact-list		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ses:ApiVersion aws:TagKeys	
UpdateConfigurationSetEventDestination	Gewährt die Berechtigung zum Aktualisieren der Konfiguration eines Ereignisziels für einen Konfigurationssatz	Schreiben	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateContact	Gewährt die Berechtigung, die Einstellungen eines Kontakts für eine Liste zu aktualisieren	Schreiben	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateContactList	Gewährt die Berechtigung zum Aktualisieren von Metadaten der Kontaktliste	Schreiben	contact-list*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateCustomVerificationEmailTemplate	Gewährt die Berechtigung zum Aktualisieren einer vorhandenen benutzerdefinierten Verifizierungs-E-Mail-Vorlage	Schreiben	custom-verification-email-template*		
				ses:ApiVersion	
UpdateEmailIdentityPolicy	Gewährt die Berechtigung zum Aktualisieren der angegebenen Sendegenehmigungsrichtlinie für die angegebene Identität (eine E-Mail-Adresse oder eine Domain)	Berechtigungsverwaltung	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateEmailTemplate	Gewährt die Berechtigung zum Aktualisieren einer E-Mail-Vorlage	Schreiben	template*		
				ses:ApiVersion	

Vom Amazon Simple Email Service v2 definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden

können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
configuration-set	`arn:${Partition}:ses:${Region}:${Account}:configuration-set/${ConfigurationSetName}`	aws:ResourceTag/${TagKey}
contact-list	`arn:${Partition}:ses:${Region}:${Account}:contact-list/${ContactListName}`	aws:ResourceTag/${TagKey}
custom-verification-email-template	`arn:${Partition}:ses:${Region}:${Account}:custom-verification-email-template/${TemplateName}`	
dedicated-ip-pool	`arn:${Partition}:ses:${Region}:${Account}:dedicated-ip-pool/${DedicatedIPPool}`	aws:ResourceTag/${TagKey}
deliverability-test-report	`arn:${Partition}:ses:${Region}:${Account}:deliverability-test-report/${ReportId}`	aws:ResourceTag/${TagKey}
export-job	`arn:${Partition}:ses:${Region}:${Account}:export-job/${ExportJobId}`	
identity	`arn:${Partition}:ses:${Region}:${Account}:identity/${IdentityName}`	aws:ResourceTag/${TagKey}
import-job	`arn:${Partition}:ses:${Region}:${Account}:import-job/${ImportJobId}`	
template	`arn:${Partition}:ses:${Region}:${Account}:template/${TemplateName}`	

Bedingungsschlüssel für Amazon Simple Email Service v2

Amazon Simple Email Service v2 definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString
ses:ApiVersion	Filtert den Zugriff nach der SES-API-Version	Zeichenfolge
ses:ExportSourceType	Filtert den Zugriff nach dem Typ der Exportquelle	Zeichenfolge
ses:FeedbackAddress	Filtert den Zugriff basierend auf der „Return-Path“-Adresse, die festlegt, wohin Unzustellbarkeitsnachrichten und Beschwerden von der Funktion für E-Mail-Feedback-Weiterleitung gesendet werden	Zeichenfolge
ses:FromAddress	Filtert den Zugriff basierend auf der „Von“-Adresse einer Nachricht	Zeichenfolge
ses:FromDisplayName	Filtert den Zugriff basierend auf der „Von“-Adresse, die als Anzeigename einer Nachricht verwendet wird	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
ses:Recipients	Filtert den Zugriff basierend auf den Empfängeradressen einer Nachricht, einschließlich der „An“-, „CC“- und „BCC“-Adressen	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Simple Workflow Service

Amazon Simple Workflow Service (Servicepräfix: `swf`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Simple Workflow Service definierte Aktionen
- Vom Amazon Simple Workflow Service definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Simple Workflow Service

Von Amazon Simple Workflow Service definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWSzu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelTimer [nur Berechtigung]	Gewährt die Berechtigung zum Abbrechen eines zuvor gestarteten Timers und zum	Schreiben	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	Aufzeichnen eines TimerCanceled Ereignisses im Verlauf				
CancelWorkflowExecution [nur Berechtigung]	Gewährt die Berechtigung zum Schließen der Workflow-Ausführung und zum Aufzeichnen eines WorkflowExecutionCanceled Ereignisses im Verlauf	Schreiben	domain*		
CompleteWorkflowExecution [nur Berechtigung]	Gewährt die Berechtigung zum Schließen der Workflow-Ausführung und zum Aufzeichnen eines WorkflowExecutionCompleted Ereignisses im Verlauf	Schreiben	domain*		
ContinueAsNewWorkflowExecution [nur Berechtigung]	Erteilt die Berechtigung, die Workflow-Ausführung zu schließen und eine neue Workflow-Ausführung desselben Typs mit derselben Workflow-ID und einer eindeutigen Ausführungs-ID zu starten	Schreiben	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CountClosedWorkflowExecutions	Erteilt die Berechtigung zum Zurückgeben der Anzahl geschlossener Workflow-Ausführungen in der gegebenen Domain, die den angegebenen Filterkriterien entsprechen	Lesen	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	
CountOpenWorkflowExecutions	Erteilt die Berechtigung zum Zurückgeben der Anzahl offener Workflow-Ausführungen in der gegebenen Domain, die den angegebenen Filterkriterien entsprechen	Lesen	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	
CountPendingActivityTasks	Erteilt die Berechtigung zum Zurückgeben der geschätzten Anzahl der Aktivitätssaufgaben in der angegebenen Aufgabenliste	Lesen	domain*		
				swf:taskList.name	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CountPendingDecisionTasks	Erteilt die Berechtigung zum Zurückgeben der geschätzten Anzahl der Entscheidungsaufgaben in der angegebenen Aufgabenliste	Lesen	domain*		
				swf:taskList.name	
DeprecateActivityType	Gewährt die Berechtigung zum Verwerten des angegebenen Aktivitätstyps	Schreiben	domain*		
				swf:activityType.name swf:activityType.version	
DeprecateDomain	Gewährt die Berechtigung zum Verwerten der angegebenen Domain	Schreiben	domain*		
DeprecateWorkflowType	Gewährt die Berechtigung zum Verwerten des angegebenen Workflow-Typs	Schreiben	domain*		
				swf:workflowType.name swf:workflowType.version	
DescribeActivityType	Gewährt die Berechtigung zum Zurückgeben von Informationen zum angegebenen Aktivitätstyp	Lesen	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				swf:activityType.name swf:activityType.version	
DescribeDomain	Gewährt die Berechtigung zum Zurückgeben von Informationen zur angegebenen Domain, einschließlich ihrer Beschreibung und Status	Lesen	domain*		
DescribeWorkflowExecution	Gewährt die Berechtigung zum Zurückgeben von Informationen zur angegebenen Workflow-Ausführung, einschließlich Typ und einiger Statistiken	Lesen	domain*		
DescribeWorkflowType	Gewährt die Berechtigung zum Zurückgeben von Informationen zum angegebenen Workflow-Typ	Lesen	domain*		
				swf:workflowType.name swf:workflowType.version	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
FailWorkflowExecution [nur Berechtigung]	Gewährt die Berechtigung zum Schließen der Workflow-Ausführung und zum Aufzeichnen eines WorkflowExecutionFailed Ereignisses im Verlauf	Schreiben	domain*		
GetWorkflowExecutionHistory	Gewährt die Berechtigung, den Verlauf der angegebenen Workflow-Ausführung zurückzugeben	Lesen	domain*		
ListActivityTypes	Erteilt die Berechtigung zum Zurückgeben der Informationen über alle in der angegebenen Domain registrierten Aktivitäten, die dem angegebenen Namen und Registrierungsstatus entsprechen	Auflisten	domain*		
ListClosedWorkflowExecutions	Erteilt die Berechtigung zum Zurückgeben einer Liste geschlossener Workflow-Ausführungen in der angegebenen Domain, die den Filterkriterien entsprechen	Auflisten	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDomains	Erteilt die Berechtigung zum Zurückgeben der Liste der im Konto registrierten Domains	Auflisten			
ListOpenWorkflowExecutions	Erteilt die Berechtigung zum Zurückgeben einer Liste offener Workflow-Ausführungen in der angegebenen Domain, die den Filterkriterien entspreche	Auflisten	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine AWS SWF-Ressource	Auflisten	domain		
ListWorkflowTypes	Gewährt die Berechtigung zum Zurückgeben von Informationen zu Workflow-Typen in der angegebenen Domain	Auflisten	domain*		
PollForActivityTask	Gewährt Auftragnehmern die Berechtigung zum Abrufen eines ActivityTask aus der angegebenen Aktivität taskList	Schreiben	domain*		
				swf:taskList.name	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PollForDecisionTask	Gewährt Entscheidern die Berechtigung zum Abrufen eines DecisionTask aus der angegebenen Entscheidungs-taskList	Schreiben	domain*		
				swf:taskList.name	
RecordActivityTaskHeartbeat	Gewährt Auftragnehmern die Berechtigung, dem Service zu melden, dass der durch das angegebene taskToken ActivityTask repräsentierte immer noch Fortschritte macht	Schreiben	domain*		
RecordMarker [nur Berechtigung]	Gewährt die Berechtigung zum Aufzeichnen eines MarkerRecorded Ereignisses im Verlauf	Schreiben	domain*		
RegisterActivityType	Erteilt die Berechtigung zum Registrieren eines neuen Aktivitätstyps zusammen mit den Konfigurationseinstellungen in der angegebenen Domain	Schreiben	domain*		
				swf:defaultTaskList.name swf:name swf:version	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RegisterDomain	Gewährt die Berechtigung zum Registrieren einer neuen Domain	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	
RegisterWorkflowType	Erteilt die Berechtigung zum Registrieren eines neuen Workflow-Typs und seiner Konfigurationseinstellungen in der angegebenen Domain	Schreiben	domain*		
				swf:defaultTaskList.name swf:name swf:version	
RequestCancelActivityTask [nur Berechtigung]	Erteilt die Berechtigung zum Versuch, eine zuvor geplante Aktivitätsaufgabe abzubrechen	Schreiben	domain*		
RequestCancelExternalWorkflowExecution [nur Berechtigung]	Erteilt die Berechtigung, eine Anforderung zum Abbrechen der angegebenen externen Workflow-Ausführung anzufordern	Schreiben	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RequestCancelWorkflowExecution	Gewährt die Berechtigung zum Aufzeichnen eines WorkflowExecutionCancelRequested Ereignisses in der aktuell ausgeführten Workflow-Ausführung, die durch die angegebene Domain, workflowId und runId identifiziert wird	Schreiben	domain*		
RespondActivityTaskCanceled	Gewährt Auftragnehmern die Berechtigung, dem Service mitzuteilen, dass das durch das taskToken ActivityTask identifizierte erfolgreich abgebrochen wurde	Schreiben	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RespondActivityTaskCompleted	Gewährt Auftragnehmern die Berechtigung, dem Service mitzuteilen, dass das durch das taskToken ActivityTask identifizierte erfolgreich mit einem Ergebnis abgeschlossen wurde (falls angegeben)	Schreiben	domain*		
				swf:activityType.name swf:activityType.version swf:tagList.member.0 swf:tagList.member.1 swf:tagList.member.2 swf:tagList.member.3 swf:tagList.member.4 swf:taskList.name	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				swf:workflowType.name swf:workflowType.version	
RespondActivityTaskFailed	Erteilt Auftragnehmern die Berechtigung, dem Service mitzuteilen, dass der durch das taskToken ActivityTask identifizierte mit Grund fehlgeschlagen ist (falls angegeben)	Schreiben	domain*		
RespondDecisionTaskCompleted	Gewährt Entscheidern die Berechtigung, dem Service mitzuteilen, dass das durch das taskToken DecisionTask identifizierte erfolgreich abgeschlossen wurde	Schreiben	domain*		
ScheduleActivityTask [nur Berechtigung]	Gewährt die Berechtigung zum Planen einer Aktivitätsaufgabe	Schreiben	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SignalExternalWorkflowExecution [nur Berechtigung]	Erteilt die Berechtigung zum Anfordern eines Signals, das an die angegebene externe Workflow-Ausführung und die angegebenen Datensätze übermittelt werden soll	Schreiben	domain*		
SignalWorkflowExecution	Gewährt die Berechtigung zum Aufzeichnen eines WorkflowExecutionSignaled Ereignisses im Verlauf der Workflow-Ausführung und zum Erstellen einer Entscheidungsaufgabe für die Workflow-Ausführung, die durch die angegebene Domain, workflowId und runId identifiziert wird	Schreiben	domain*		
StartChildWorkflowExecution [nur Berechtigung]	Erteilt die Berechtigung, die Ausführung eines untergeordneten Workflows anzufordern	Schreiben	domain*		
StartTimer [nur Berechtigung]	Gewährt die Berechtigung zum Starten eines Timers für eine Workflow-Ausführung	Schreiben	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartWorkflowExecution	Erteilt die Berechtigung zum Starten einer Ausführung des Workflow-Typs in der angegebenen Domain unter Verwendung der übergebenen workflowId und Eingabedaten	Schreiben	domain*	swf:tagList.member.0 swf:tagList.member.1 swf:tagList.member.2 swf:tagList.member.3 swf:tagList.member.4 swf:taskList.name swf:workflowType.name swf:workflowType.version	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Markieren einer AWS SWF-Ressource	Tagging	domain		
				aws:TagKeys aws:RequestTag/${TagKey}	
TerminateWorkflowExecution	Gewährt die Berechtigung zum Aufzeichnen eines WorkflowExecutionTerminated Ereignisses und zum Erzwingen des Schließens der Workflow-Ausführung, die durch die angegebene Domain, runId und workflowId identifiziert ist	Schreiben	domain*		
UndeprecateActivityType	Erteilt die Berechtigung zum Aufheben der Erkennung eines zuvor veralteten Aktivitätstyps	Schreiben	domain*		
				swf:activityType.name swf:activityType.version	
UndeprecateDomain	Erteilt die Berechtigung zum Aufheben der Erkennung einer zuvor veralteten Domain	Schreiben	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UndeprecateWorkflowType	Erteilt die Berechtigung zum Aufheben der Erkennung eines zuvor veralteten Workflow-Typs	Schreiben	domain*		
				swf:workflowType.name swf:workflowType.version	
UntagResource	Gewährt die Berechtigung zum Entfernen eines Tags aus einer AWS SWF-Ressource	Tagging	domain		
				aws:TagKeys	

Vom Amazon Simple Workflow Service definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
domain	`arn:${Partition}:swf::${Account}:/domain/${DomainName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Simple Workflow Service

Amazon Simple Workflow Service definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tag der Anforderung	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach Tag der Ressource	String
aws:TagKeys	Filtert den Zugriff nach Tag des Schlüssels	ArrayOfString
swf:activityType.name	Filtert den Zugriff nach dem Namen des Aktivitätstyps	String
swf:activityType.version	Filtert den Zugriff nach der Version des Aktivitätstyps	String
swf:defaultTaskList.name	Filtert den Zugriff nach dem Namen der Standardaufgabenliste	String
swf:name	Filtert den Zugriff nach dem Namen von Aktivitäten oder Workflows	String
swf:tagFilter.tag	Filtert den Zugriff nach dem Wert des tagFilter.tag	String
swf:tagList.member.0	Filtert den Zugriff nach dem angegebenen Tag	String

Bedingungsschlüssel	Beschreibung	Typ
swf:tagList.member.1	Filtert den Zugriff nach dem angegebenen Tag	String
swf:tagList.member.2	Filtert den Zugriff nach dem angegebenen Tag	String
swf:tagList.member.3	Filtert den Zugriff nach dem angegebenen Tag	String
swf:tagList.member.4	Filtert den Zugriff nach dem angegebenen Tag	String
swf:taskList.name	Filtert den Zugriff nach dem Namen der Aufgabenliste	String
swf:typeFilter.name	Filtert den Zugriff nach dem Namen des Typfilters	String
swf:typeFilter.version	Filtert den Zugriff nach der Version des Typfilters	String
swf:version	Filtert den Zugriff nach der Version von Aktivitäten oder Workflows	String
swf:workflowType.name	Filtert den Zugriff nach dem Namen des Workflow-Typs	String
swf:workflowType.version	Filtert den Zugriff nach der Version des Workflow-Typs	String

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon SimpleDB

Amazon SimpleDB (Servicepräfix: `sdb`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon SimpleDB definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchDeleteAttributes	Führt mehrere DeleteAttributes-Produktionen in einem Aufruf aus, um Netzläufe und Latenzen zu reduzieren	Schreiben	domain*		
BatchPutAttributes	Mit der Produktion BatchPutAttributes können Sie mehrere PutAttribute-Produktionen in nur einem Aufruf ausführen. Mit der Produktion BatchPutAttributes können Sie mehrere PutAttribute-Produktionen in nur einem Aufruf ausführen	Schreiben	domain*		
CreateDomain	Die Produktion CreateDomain erstellt eine neue Domain	Schreiben	domain*		
DeleteAttributes	Löscht einzelne oder mehrere Attribute, die dem Element zugeordnet sind	Schreiben	domain*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteDomain	Die Produktion DeleteDomain löscht eine Domain	Schreiben	domain*		
DomainMetadata	Gibt Informationen zur Domain zurück: wann die Domain erstellt wurde, die Anzahl der Elemente und Attribute und die Größe der Attributnamen und -werte	Lesen	domain*		
GetAttributes	Gibt alle Attribute zurück, die dem Element zugeordnet sind	Lesen	domain*		
ListDomains	Beschreibung für ListDomains	Auflisten			
PutAttributes	Die Produktion PutAttributes erstellt oder ersetzt Attribute in einem Element	Schreiben	domain*		
Select	Beschreibung für Select	Read	domain*		

Von Amazon SimpleDB definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressource ntypen	ARN	Bedingungsschlüssel
domain	`arn:${Partition}:sdb:${Region}:${Account}:domain/${DomainName}`	

Bedingungsschlüssel für Amazon SimpleDB

SimpleDB besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS SimSpace Weaver

AWS SimSpace Weaver (Service-Präfix: `simspaceweaver`) bietet die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS SimSpace Weaver definierte Aktionen
- Von AWS SimSpace Weaver definierte Ressourcentypen
- Bedingungsschlüssel für AWS SimSpace Weaver

Von AWS SimSpace Weaver definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen.

Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSnapshot	Gewährt die Berechtigung zum Erstellen eines Snapshots	Schreiben	Simulation*		
DeleteApp	Gewährt die Berechtigung zum Löschen einer App	Schreiben	Simulation*		
DeleteSimulation	Gewährt die Berechtigung zum Löschen einer Simulation	Schreiben	Simulation*		
DescribeApp	Gewährt die Berechtigung zur Beschreibung einer App	Lesen	Simulation*		
DescribeSimulation	Gewährt die Berechtigung zum Beschreiben einer Simulation	Lesen	Simulation*		
ListApps	Gewährt die Berechtigung zum Auflisten von Apps	Lesen	Simulation*		
ListSimulations	Gewährt die Berechtigung zum Auflisten von Simulation	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für eine Ressource	Lesen			
StartApp	Gewährt die Berechtigung zum Starten einer Anwendung	Schreiben	Simulation*		
StartClock	Gewährt die Berechtigung zum Starten einer Simulationsuhr	Schreiben	Simulation*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartSimulation	Gewährt die Berechtigung zum Starten eines Multiplexes	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
StopApp	Gewährt die Berechtigung zum Beenden einer Anwendung	Schreiben	Simulation*		
StopClock	Gewährt die Berechtigung zum Anhalten einer Simulationsuhr	Schreiben	Simulation*		
StopSimulation	Gewährt die Berechtigung zum Stoppen eines Multiplexes	Schreiben	Simulation*		
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren	Simulation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Markierung	Simulation*		
				aws:TagKeys	

Von AWS SimSpace Weaver definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Simulation	`arn:${Partition}:simspaceweaver:${Region}:${Account}:simulation/${SimulationName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS SimSpace Weaver

AWS SimSpace Weaver definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch Tags, die in der Anforderung übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf Tags, die der Ressource zugeordnet sind	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert den Zugriff basierend auf Tag-Schlüsseln, die in der Anforderung übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Snow Device Management

AWS Snow Device Management (Servicepräfix: `snow-device-management`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von definierte AktionenAWSSnow Device Management
- Von AWS Snow Device Management definierte Ressourcentypen
- Bedingungsschlüssel fürAWSSnow Device Management

Von definierte AktionenAWSSnow Device Management

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelTask	Gewährt die Berechtigung zum Abbrechen von Aufgaben auf Remotegeräten	Schreiben	task*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateTask	Gewährt die Berechtigung zum Erstellen von Aufgaben auf Remotegeräten	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DescribeDevice	Gewährt die Berechtigung zum Beschreiben eines fernverwalteten Geräts	Lesen	managed-device*		
DescribeDeviceEc2Instances	Gewährt die Berechtigung zum Beschreiben der EC2-Instanzen eines remote verwalteten Geräts	Lesen	managed-device*		
DescribeExecution	Gewährt die Berechtigung zum Beschreiben einer Ausführung	Lesen			
DescribeTask	Gewährt die Berechtigung, einen Ledger zu beschreiben	Lesen	task*		
ListDeviceResources	Gewährt die Berechtigung zum Auflisten der Ressourcen eines remote verwalteten Geräts	Auflisten	managed-device*		
ListDevices	Gewährt die Berechtigung zum Auflisten von remote verwalteten Geräten	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListExecutions	Gewährt die Berechtigung zum Auflisten ausgeführter Synchronisierungsaufgaben	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für eine Ressource (Gerät oder Aufgabe)	Lesen		aws:RequestTag/${TagKey} aws:TagKeys	
ListTasks	Gewährt die Berechtigung zum Auflisten aller Komponenten	Auflisten			
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markieren	managed-device		
			task		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Ressource	Markierung	managed-device		
			task		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	

Von AWS Snow Device Management definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
managed-device	`arn:${Partition}:snow-device-management:${Region}:${Account}:managed-device/${ResourceId}`	aws:ResourceTag/${TagKey}
task	`arn:${Partition}:snow-device-management:${Region}:${Account}:task/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel fürAWSSnow Device Management

AWS Snow Device Management definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um

die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Zugriff basierend auf dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung.	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tag-Schlüssel-Wert-Paaren, die an die Ressource angefügt wurden	Zeichenfolge
aws:TagKeys	Filtert Zugriff basierend auf dem Vorhandensein von Tag-Schlüsseln in der Anforderung.	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Snowball

AWS Snowball (Servicepräfix: `snowball`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Snowball definierte Aktionen
- Von AWS Snowball definierte Ressourcentypen
- Bedingungsschlüssel für AWS Snowball

Von AWS Snowball definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelCluster	Gewährt die Berechtigung zum Abbrechen einer Cluster-Aufgabe	Schreiben			
CancelJob	Gewährt die Berechtigung zum Abbrechen des angegebenen Auftrags	Schreiben			
CreateAddress	Gewährt die Berechtigung zum Erstellen einer Adresse, an die ein Snowball versendet werden soll	Schreiben			
CreateCluster	Gewährt die Berechtigung zum Erstellen eines leeren Clusters	Schreiben			
CreateJob	Gewährt die Berechtigung zum Erstellen eines Auftrags zum Importieren oder Exportieren von Daten zwischen Amazon S3 und Ihrem On-Premises-Rechenzentrum	Schreiben			
CreateLongTermPricing	Gewährt die Berechtigung, einen LongTermPricingListEntry zu erstellen, damit Kunden einen Vertrag zur Vorausabrechnung für einen Auftrag hinzufügen können	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateReturnShippingLabel	Gewährt die Berechtigung zum Erstellen eines Versandetiketts, mit dem das Snow-Gerät an AWS zurückgesendet wird	Schreiben			
DescribeAddress	Gewährt die Berechtigung zum Abrufen spezifischer Details zu dieser Adresse in Form eines Adressobjekts	Lesen			
DescribeAddresses	Gewährt die Berechtigung zum Beschreiben einer angegebenen Anzahl von ADRESS-Objekten	Auflisten			
DescribeCluster	Gewährt die Berechtigung zum Beschreiben der Informationen zu einem bestimmten Cluster, einschließlich Versandinformationen, Cluster-Status sowie weiterer wichtiger Metadaten	Lesen			
DescribeJob	Gewährt die Berechtigung zum Beschreiben der Informationen zu einem bestimmten Auftrag, einschließlich Versandinformationen, Auftragsstatus sowie weiterer wichtiger Metadaten	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeReturnShippingLabel	Gewährt die Berechtigung zum Beschreiben der Informationen auf dem Versandetikett eines Snow-Geräts, das an AWS zurückgesendet wird	Lesen			
GetJobManifest	Gewährt die Berechtigung zum Abrufen eines Links zu einer vorsignierten Amazon-S3-URL für die Manifestdatei, die dem angegebenen JobId-Wert zugeordnet ist	Lesen			
GetJobUnlockCode	Gewährt die Berechtigung zum Abrufen des UnlockCode-Werts für den angegebenen Auftrag	Lesen			
GetSnowballUsage	Gewährt die Berechtigung zum Abrufen von Informationen zum Snowball-Serviceli mit für Ihr Konto sowie zu der Anzahl an Sowballs, die Ihr Konto verwendet	Lesen			
GetSoftwareUpdates	Gewährt die Berechtigung zum Zurückgeben einer vorsignierten Amazon-S3-URL für eine Aktualisierungsdatei, die einer angegebenen JobId zugeordnet ist	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListClusterJobs	Gewährt die Berechtigung zum Auflisten von JobListEntry-Objekten der angegebenen Länge	Auflisten			
ListClusters	Gewährt die Berechtigung zum Auflisten von ClusterListEntry-Objekten der angegebenen Länge	Auflisten			
ListCompatibleImages	Gewährt die Berechtigung zum Zurückgeben einer Liste der Amazon Machine Images (AMIs) von Amazon EC2, die Ihrem AWS-Konto gehören und deren Verwendung auf einem Snow-Gerät unterstützt würde	Auflisten			
ListJobs	Gewährt die Berechtigung zum Auflisten von JobListEntry-Objekten der angegebenen Länge	Auflisten			
ListLongTermPricing	Gewährt die Berechtigung zum Auflisten von LongTermPricingListEntry-Objekten für das Konto, das die Anfrage stellt	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListPickupLocations	Gewährt die Berechtigung zum Auflisten von Adressobjekten mit der angegebenen Länge, bei denen eine Abholung verfügbar ist	Auflisten			
ListServiceVersions	Gewährt die Berechtigung zum Auflisten aller unterstützten Versionen für die On-Device-Services von Snow	Auflisten			
UpdateCluster	Gewährt die Berechtigung zum Aktualisieren einiger einem Cluster zugeordneter Informationen, während der ClusterState-Wert eines Clusters im AwaitingQuorum-Status ist	Schreiben			
UpdateJob	Gewährt die Berechtigung zum Aktualisieren einiger einem Auftrag zugeordneter Informationen, während der JobState-Wert eines Auftrags „New“ lautet	Schreiben			
UpdateJobShipmentState	Gewährt die Berechtigung zum Aktualisieren des Status, wenn der Status einer Sendung sich ändert	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateLongTermPricing	Gewährt die Berechtigung zum Aktualisieren eines bestimmten Vertrages zur Vorausabrechnung für einen Auftrag	Schreiben			

Von AWS Snowball definierte Ressourcentypen

AWS Snowball unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf AWS Snowball zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Snowball

Snowball besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon SNS

Amazon SNS (Servicepräfix: `sns`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon SNS definierte Aktionen

- Von Amazon SNS definierte Ressourcentypen
- Bedingungsschlüssel für Amazon SNS

Von Amazon SNS definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddPermission	Gewährt die Berechtigung zum Hinzufügen einer Anweisung zu der Zugriffsrichtlinie für ein Thema, die Zugriff auf die angegebenen AWS-Konten für die angegebene Aktionen Gewährt	Berechtigungsverwaltung	topic*		
CheckIfPhoneNumberIsOptedOut	Gewährt die Berechtigung zum Akzeptieren einer Telefonnummer und gibt an, ob der Telefoninhaber sich vom Empfang von SMS-Nachrichten von Ihrem Konto abgemeldet hat	Read			
ConfirmSubscription	Gewährt die Berechtigung zum Überprüfen der Absicht des Eigentümers eines Endpunkts, Nachrichten zu empfangen, indem Sie das Token auswerten, das dem Endpunkt in einer früheren Subscribe-Aktion gesendet wurde	Write	topic*		
CreatePlatformApplication	Gewährt die Berechtigung zum Erstellen eines Plattform anwendungsobjekt für einen unterstützten Push-Bena	Write			iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	chrichtigungsservice (z. B. APNS und GCM), bei dem sich Geräte und mobile Apps registrieren können				
CreatePlatformEndpoint	Gewährt die Berechtigung zum Erstellen eines Endpunkts für ein Gerät und eine mobile App für einen unterstützten Push-Benachrichtigungsservice wie APNS und GCM	Write			
CreateSMSSandboxPhoneNumber	Gewährt die Berechtigung zum Hinzufügen einer Zielrufnummer und zum Senden eines Einmalpasswort (OTP) für ein AWS-Konto an diese Telefonnummer	Write			
CreateTopic	Gewährt die Berechtigung zum Erstellen eines Themas, für das Benachrichtigungen veröffentlicht werden können	Write	topic*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteEndpoint	Gewährt die Berechtigung zum Löschen des Endpunkts für ein Gerät und eine mobile App von Amazon SNS	Write			
DeletePlatformApplication	Gewährt die Berechtigung zum Löschen eines Plattform anwendungsobjekt eines unterstützten Push-Benachrichtigungsservices wie APNS oder GCM	Write			
DeleteSMSSandboxPhoneNumber	Gewährt die Berechtigung zum Löschen der verifizierten oder ausstehenden Telefonnummer eines AWS-Konto	Write			
DeleteTopic	Gewährt die Berechtigung zum Löschen eines Themas und aller seiner Abonnements	Schreiben	topic*		
GetDataProtectionPolicy	Erteilt die Erlaubnis zur Rückgabe der Datenschutzerklärung des Themas	Lesen	topic*		
GetEndpointAttributes	Gewährt die Berechtigung zum Abrufen der Endpunktattribute für ein Gerät eines unterstützten Push-Benachrichtigungsservices wie APNS oder GCM	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetPlatformApplicationAttributes	Gewährt die Berechtigung zum Abrufen der Attribute des Plattformanwendungsobjekts für die unterstützten Push-Benachrichtigungsservices wie APNS und GCM	Read			
GetSMSAttributes	Gewährt die Berechtigung zum Zurückgeben der Einstellungen für das Senden von SMS-Nachrichten von Ihrem Konto	Read			
GetSMSSandboxAccountStatus	Gewährt die Berechtigung zum Abrufen des Sandbox-Status für das aufrufende Konto in der Zielregion	Read			
GetSubscriptionAttributes	Gewährt die Erlaubnis zum Zurückgeben aller Eigenschaften eines Abonnements	Read			
GetTopicAttributes	Gewährt die Erlaubnis zum Zurückgeben aller Eigenschaften eines Themas	Read	topic*		
ListEndpointsByPlatformApplication	Gewährt die Berechtigung zum Auflisten der Endpunkte und Endpunktattribute für Geräte in einem unterstützten Push-Benachrichtigungsservice wie GCM oder APNS	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListOriginationNumbers	Gewährt die Erlaubnis zum Auflisten aller Ursprungsnummern und ihrer Metadaten	List			
ListPhoneNumbersOptedOut	Gewährt die Berechtigung zum Zurückgeben einer Liste der Telefonnummern, die sich vom Nachrichtenempfang abgemeldet haben, an die Sie also keine SMS-Nachrichten senden können	Read			
ListPlatformApplications	Gewährt die Berechtigung zum Auflisten der Plattform anwendungsobjekte für die unterstützten Push-Benachrichtigungsservices wie APNS und GCM	List			
ListSMSSandboxPhoneNumbers	Gewährt die Berechtigung zum Auflisten der aktuellen ausstehenden und verifizierten Zielrufnummern des anrufenden Kontos	List			
ListSubscriptions	Gewährt die Erlaubnis zum Zurückgeben einer Liste der Abonnements des Auftraggebers	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListSubscriptionsByTopic	Gewährt die Berechtigung zum Abrufen einer Liste aller Abonnements für ein bestimmtes Thema	List	topic*		
ListTagsForResource	Gewährt die Berechtigung zum Auflisten aller Tags, die zum angegebenen Amazon-SNS-Thema hinzugefügt wurden	Read	topic		
ListTopics	Gewährt die Erlaubnis zum Zurückgeben einer Liste der Themen des Auftraggebers	List			
OptInPhoneNumber	Gewährt die Berechtigung zum Anmelden einer derzeit abgemeldeten Telefonnummer für den Empfang von Nachrichten, damit Sie wieder SMS-Nachrichten an die Nummer senden können	Write			
Publish	Gewährt die Berechtigung zum Senden einer Nachricht an alle abonnierten Endpunkte eines Themas	Schreiben	topic*		
PutDataProtectionPolicy	Gewährt die Berechtigung, einem Themenbesitzer zu erlauben, die Datenschutzrichtlinie festzulegen	Schreiben	topic*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RemovePermission	Gewährt die Berechtigung zum Entfernen einer Anweisung aus der Zugriffssteuerungsrichtlinie eines Themas	Berechtigungsverwaltung	topic*		
SetEndpointAttributes	Gewährt die Berechtigung zum Festlegen der Attribute für einen Endpunkt für ein Gerät eines unterstützten Push-Benachrichtigungsservices wie GCM oder APNS	Write			
SetPlatformApplicationAttributes	Gewährt die Berechtigung zum Festlegen der Attribute des Plattformanwendung sobjekts für die unterstützten Push-Benachrichtigungsservices wie APNS und GCM	Write			iam:PassRole
SetSMSAttributes	Gewährt die Berechtigung zum Festlegen der Standardeinstellungen für das Senden von SMS-Nachrichten und den Empfang täglicher SMS-Nutzungsberichte	Write			
SetSubscriptionAttributes	Gewährt die Berechtigung, einem Abonnementbesitzer zu erlauben, ein Attribut des Themas auf einen neuen Wert festzulegen	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SetTopicAttributes	Gewährt die Berechtigung, einem Themenbesitzer zu erlauben, ein Attribut des Themas auf einen neuen Wert festzulegen	Berechtigungsverwaltung	topic*		iam:PassRole
Subscribe	Gewährt die Berechtigung, sich auf das Abonnieren eines Endpunkts vorzubereiten, indem dem Endpunkt eine Bestätigungsnachricht gesendet wird	Write	topic*		
				sns:Endpoint sns:Protocol	
TagResource	Gewährt die Erlaubnis zum Hinzufügen von Tags zum angegebenen Amazon-SNS-Thema	Markieren	topic		
				aws:RequestTag/${TagKey} aws:TagKeys	
Unsubscribe	Gewährt die Berechtigung zum Löschen eines Abonnements	Write			
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags von dem angegebenen Amazon-SNS-Themas	Markieren	topic		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
VerifySMSSandboxPhoneNumber	Gewährt die Berechtigung zum Überprüfen einer Ziel-Telefonnummer mit einem Einmalpasswort (OTP) für ein AWS-Konto	Write			

Von Amazon SNS definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
topic	`arn:${Partition}:sns:${Region}:${Account}:${TopicName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon SNS

Amazon SNS definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tags aus der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf Tags, die der Ressource zugeordnet sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach Tag-Schlüsseln aus der Anforderung	ArrayOfString
sns:Endpoint	Filtert den Zugriff nach der URL, der E-Mail-Adresse oder dem ARN aus einer Subscribe-Anforderung oder einem zuvor bestätigten Abonnement	Zeichenfolge
sns:Protocol	Filtert den Zugriff nach dem Protokollwert aus einer Subscribe-Anforderung oder einem zuvor bestätigten Abonnement	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für AWS SQL Workbench

AWS SQL Workbench (Service-Präfix: `sqlworkbench`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS SQL Workbench definierte Aktionen
- Von AWS SQL Workbench definierte Ressourcentypen
- Bedingungsschlüssel für AWS SQL Workbench

Von AWS SQL Workbench definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateConnectionWithChart [nur Berechtigung]	Gewährt die Berechtigung zum Zuordnen einer Verbindung zu einem Diagramm	Schreiben	chart*		
			connection*		
AssociateConnectionWithTab [nur Berechtigung]	Gewährt die Berechtigung zum Zuordnen einer Verbindung zu einem Tab	Schreiben	connection*		
AssociateNotebookWithTab [nur Berechtigung]	Gewährt die Berechtigung zum Zuordnen eines Notebook zu einem Tab	Schreiben	notebook*		
AssociateQueryWithTab [nur Berechtigung]	Gewährt die Berechtigung zum Zuordnen einer Abfrage zu einem Tab	Schreiben	query*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchDeleteFolder [nur Berechtigung]	Gewährt die Berechtigung zum Löschen von Ordnern in Ihrem Konto	Schreiben			
BatchGetNotebookCell [nur Berechtigung]	Erteilt die Berechtigung zum Abrufen von Notizbuch zelleninhalten in Ihrem Konto	Lesen	notebook*		
CreateAccount [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines SQLWorkbench-Kontos	Schreiben			
CreateChart [nur Berechtigung]	Gewährt die Berechtigung, ein neues gespeichertes Diagramm in Ihrem Konto zu erstellen	Schreiben	chart*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateConnection [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer neuen Verbindung in Ihrem Konto	Schreiben	connection*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateFolder [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines Ordners in Ihrem Konto	Schreiben			
CreateNotebook [nur Berechtigung]	Erteilt die Berechtigung zum Erstellen eines neuen Notizbuchs in Ihrem Konto	Schreiben	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateNotebookCell [nur Berechtigung]	Erteilt die Berechtigung zum Erstellen einer Notizbuchzelle in Ihrem Konto	Schreiben	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateNotebookFromVersion [nur Berechtigung]	Erteilt die Berechtigung zum Erstellen eines neuen Notizbuchs aus einer Notizbuchversion in Ihrem Konto	Schreiben	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateNotebookVersion [nur Berechtigung]	Erteilt die Berechtigung zum Erstellen einer Notebook-Version für Ihr Konto	Schreiben	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateSavedQuery [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer neuen gespeicherten Abfrage in Ihrem Konto	Schreiben	query*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteChart [nur Berechtigung]	Gewährt die Berechtigung zum Entfernen von Diagrammen in Ihrem Konto	Schreiben	chart*		
DeleteConnection [nur Berechtigung]	Gewährt die Berechtigung zum Entfernen von Verbindungen in Ihrem Konto	Schreiben	connection*		
DeleteNotebook [nur Berechtigung]	Erteilt die Berechtigung zum Entfernen von Notizbüchern in Ihrem Konto	Schreiben	notebook*		
DeleteNotebookCell [nur Berechtigung]	Erteilt die Berechtigung zum Entfernen von Notizbuchzellen in Ihrem Konto	Schreiben	notebook*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteNotebookVersion [nur Berechtigung]	Erteilt die Berechtigung zum Entfernen von Notizbuchzellen in Ihrem Konto	Schreiben	notebook*		
DeleteSavedQuery [nur Berechtigung]	Gewährt die Berechtigung zum Entfernen gespeicherter Abfragen in Ihrem Konto	Schreiben	query*		
DeleteTab [nur Berechtigung]	Gewährt die Berechtigung zum Entfernen eines Tabs aus Ihrem Konto	Schreiben			
DriverExecute [nur Berechtigung]	Gewährt die Berechtigung zum Ausführen einer Abfrage in Ihrem Redshift-Cluster	Schreiben	connection*		
DuplicateNotebook [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen eines neuen Notizbuches durch Duplizieren eines vorhandenen Notizbuches in Ihrem Konto	Schreiben	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ExportNotebook [nur Berechtigung]	Erteilt die Berechtigung zum Exportieren eines Notizbuchs in Ihr Konto	Lesen	notebook*		
GenerateSession [nur Berechtigung]	Gewährt die Berechtigung, eine neue Sitzung in Ihrem Konto zu erstellen	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAccountInfo [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Kontoinformationen	Lesen			
GetAccountSettings [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Konto-Einstellungen	Lesen			
GetAutocompletionMetadata [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen der Datenbankstrukturmetadaten für automatisches Fertigstellen	Lesen			
GetAutocompletionResource [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen der Datenbankstrukturinformationen für automatisches Fertigstellen	Lesen			
GetChart [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Diagrammen für Ihr Konto	Lesen	chart*		
GetConnection [nur Berechtigung]	Gewährt die Berechtigung, Verbindungen für Ihr Konto herzustellen	Lesen	connection*		
GetNotebook [nur Berechtigung]	Gewährt die Berechtigung, Notebook-Metadaten für Ihr Konto herzustellen	Lesen	notebook*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetNotebookVersion [nur Berechtigung]	Erteilt die Berechtigung, den Inhalt einer Notebook-Version in Ihrem Konto abzurufen	Lesen	notebook*		
GetQSqlRecommendations [nur Berechtigung]	Gewährt die Berechtigung, Text-to-SQL-Empfehlungen zu erhalten	Lesen			
GetQueryExecutionHistory [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen der Abfrageausführung in Ihrem Konto.	Lesen			
GetSavedQuery [nur Berechtigung]	Gewährt die Berechtigung, gespeicherte Abfragen für Ihr Konto abzurufen	Lesen	query*		
GetSchemaInference [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen der aus einer Datei abgeleiteten Spalten und Datentypen	Lesen			
GetUserInfo [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Benutzerinformationen	Lesen			
GetUserWorkspaceSettings [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Workspace-Einstellungen für Ihr Konto	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ImportNotebook [nur Berechtigung]	Gewährt die Berechtigung zum Importieren eines Notizbuchs in Ihr Konto	Schreiben	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ListConnections [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der Verbindungen in Ihrem Konto	Auflisten			
ListDatabases [nur Berechtigung]	Gewährt die Berechtigung, Datenbanken Ihres Redshift-Clusters aufzulisten	Auflisten			
ListFiles [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Dateien und Ordnern	Auflisten			
ListNotebookVersions [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Metadaten für Ihr Konto	Auflisten	notebook*		
ListNotebooks [nur Berechtigung]	Erteilt die Berechtigung zum Auflisten der Notizbücher in Ihrem Konto	Auflisten			
ListQueryExecutionHistory [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten des Abfrageausführungsverlaufs in Ihrem Konto.	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListRedshiftClusters [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Redshift-Clustern in Ihrem Konto	Auflisten			
ListSampleDatabases [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Beispieldatenbanken	Lesen			
ListSavedQueryVersions [nur Berechtigung]	Gewährt die Berechtigung zur Auflistung von Versionen gespeicherter Abfragen in Ihrem Konto	Auflisten	query*		
ListTabs [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Tabs in Ihrem Konto	Auflisten			
ListTaggedResources [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten markierter Ressourcen	Lesen			
ListTagsForResource [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der Tags einer sqlworkbench-Ressource	Lesen	chart		
			connection		
			notebook		
			query		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutTab [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen oder Aktualisieren eines Tabs in Ihrem Konto	Schreiben			
PutUserWorkspaceSettings [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren von Workspace-Einstellungen in Ihrem Konto	Schreiben			
RestoreNotebookVersion [nur Berechtigung]	Erteilt die Berechtigung zum Wiederherstellen eines Notizbuchs in Ihrem Konto auf eine Version	Schreiben	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource [nur Berechtigung]	Gewährt die Berechtigung zum Markieren einer sqlworkbench-Ressource	Markierung	chart		
			connection		
			notebook		
			query		
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UntagResource [nur Berechtigung]	Gewährt die Berechtigung zum Aufheben der Markierung einer sqlworkbench-Ressource	Markierung	chart		
			connection		
			notebook		
			query		
				aws:TagKeys	
UpdateAccountConnectionSettings [nur Berechtigung]	Erteilung der Berechtigung zur Aktualisierung der kontoweiten Verbindungseinstellungen	Schreiben			
UpdateAccountExportSettings [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren der Exporteinstellungen für das gesamte Konto.	Schreiben			
UpdateAccountGeneralSettings [nur Berechtigung]	Erteilung der Berechtigung zur Aktualisierung kontoweiter allgemeiner Einstellungen	Schreiben			
UpdateAccountQSqlSettings [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren von text-to-SQL-Einstellungen für das gesamte Konto	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateChart [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren eines Diagramms in Ihrem Konto	Schreiben	chart*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateConnection [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren einer Verbindung in Ihrem Konto	Schreiben	connection*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateFileFolder [nur Berechtigung]	Gewährt die Berechtigung zum Verschieben von Dateien in Ihrem Konto	Schreiben	chart		
			query		
UpdateFolder [nur Berechtigung]	Gewährt die Berechtigung, den Namen und die Details eines Ordners in Ihrem Konto zu aktualisieren	Schreiben			
UpdateNotebook [nur Berechtigung]	Erteilt die Berechtigung zum Aktualisieren von Notizbuch metadaten in Ihrem Konto	Schreiben	notebook*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateNotebookCellContent [nur Berechtigung]	Erteilt die Berechtigung zum Aktualisieren eines Notizbuch zelleninhalts in Ihrem Konto	Schreiben	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateNotebookCellLayout [nur Berechtigung]	Erteilt die Berechtigung zum Aktualisieren eines Notizbuch zellen-Layouts in Ihrem Konto	Schreiben	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateSavedQuery [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren einer gespeicherten Abfrage in Ihrem Konto	Schreiben	query*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Von AWS SQL Workbench definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
connection	`arn:${Partition}:sqlworkbench:${Region}:${Account}:connection/${ResourceId}`	aws:ResourceTag/${TagKey}
query	`arn:${Partition}:sqlworkbench:${Region}:${Account}:query/${ResourceId}`	aws:ResourceTag/${TagKey}
chart	`arn:${Partition}:sqlworkbench:${Region}:${Account}:chart/${ResourceId}`	aws:ResourceTag/${TagKey}
notebook	`arn:${Partition}:sqlworkbench:${Region}:${Account}:notebook/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS SQL Workbench

AWS SQL Workbench definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon SQS

Amazon SQS (Servicepräfix: `sqs`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon SQS definierte Aktionen
- Von Amazon SQS definierte Ressourcentypen
- Bedingungsschlüssel für Amazon SQS

Von Amazon SQS definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den

Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddPermission	Gewährt einer Warteschlange die Berechtigung für einen bestimmten Prinzipal	Berechtigungsverwaltung	queue*		
CancelMessageMoveTask	Gewährt die Berechtigung zum Abbrechen einer laufenden Aufgabe zum Verschieben von Nachrichten	Schreiben	queue*		
ChangeMessageVisibility	Gewährt die Berechtigung, die Zeitbeschränkung für die Sichtbarkeit einer bestimmten Nachricht in einer Warteschlange auf einen neuen Wert zu ändern	Schreiben	queue*		
CreateQueue	Gewährt die Berechtigung zum Erstellen einer neuen Warteschlange oder gibt die URL einer vorhandenen Warteschlange zurück	Schreiben	queue*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteMessage	Gewährt die Berechtigung, die angegebene Nachricht aus der angegebenen Warteschlange zu löschen	Schreiben	queue*		
DeleteQueue	Gewährt die Berechtigung zum Löschen der durch die Warteschlangen-URL	Schreiben	queue*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	angegebenen Warteschlange, unabhängig davon, ob die Warteschlange leer ist				
GetQueueAttributes	Gewährt die Berechtigung zum Abrufen von Attributen für die angegebene Warteschlange	Lesen	queue*		
GetQueueUrl	Gewährt die Berechtigung, die URL einer vorhandenen Warteschlange zurückzugeben	Lesen	queue*		
ListDeadLetterSourceQueues	Gewährt die Berechtigung, eine Liste der Warteschlangen zurückzugeben, die das RedrivePolicy-Wartschlangenattribut mit einer Warteschlange für unzustellbare Nachrichten konfiguriert haben	Lesen	queue*		
ListMessageMoveTasks	Gewährt die Berechtigung zum Auflisten von Aufgaben zum Verschieben von Nachrichten	Lesen	queue*		
ListQueueTags	Gewährt die Berechtigung zum Auflisten von Tags, die zu einer SQS-Warteschlange hinzugefügt wurden	Lesen	queue*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListQueues	Gewährt die Berechtigung, eine Liste der Warteschlangen zurückzugeben	Lesen			
PurgeQueue	Gewährt die Berechtigung zum Löschen der Nachrichten in einer Warteschlange, die durch die Warteschlangen-URL angegeben ist	Schreiben	queue*		
ReceiveMessage	Gewährt die Berechtigung zum Abrufen einer oder mehrerer Nachrichten (maximal 10 Nachrichten) aus der angegebenen Warteschlange	Lesen	queue*		
RemovePermission	Gewährt die Berechtigung, alle Berechtigungen in der Warteschlangenrichtlinie zu widerrufen, die dem angegebenen Label-Parameter entsprechen	Berechtigungsverwaltung	queue*		
SendMessage	Gewährt die Berechtigung, eine Nachricht an die angegebene Warteschlange zuzustellen	Schreiben	queue*		
SetQueueAttributes	Gewährt die Berechtigung zum Festlegen des Werts eines oder mehrerer Warteschlangenattribute	Schreiben	queue*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartMessageMoveTask	Gewährt die Berechtigung zum Beginnen einer Aufgabe zum Verschieben von Nachrichten	Schreiben	queue*		
TagQueue	Gewährt die Berechtigung zum Hinzufügen von Tags zur angegebenen SQS-Warteschlange	Markierung	queue*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagQueue	Gewährt die Berechtigung zum Entfernen von Tags aus der angegebenen SQS-Warteschlange	Markierung	queue*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Von Amazon SQS definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types (Ressourcen-Typen).

> **Note**
>
> Der ARN der Warteschlange wird nur in IAM-Berechtigungsrichtlinien verwendet. In API- und CLI-Aufrufen verwenden Sie stattdessen die URL der Warteschlange.

Ressourcentypen	ARN	Bedingungsschlüssel
queue	`arn:${Partition}:sqs:${Region}:${Account}:${QueueName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon SQS

Amazon SQS definiert die folgenden Bedingungsschlüssel, die in einem `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Step Functions

AWS Step Functions (Dienstpräfix:`states`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Step Functions definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateActivity	Gewährt die Berechtigung zum Erstellen einer Aktivität	Write	activity*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStateMachine	Gewährt die Berechtigung zum Erstellen eines Zustandsautomaten	Schreiben	statemachine*		iam:PassRole states:PublishStat

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					eMachineVersion
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStateMachineAlias	Gewährt die Berechtigung, einen Zustandsautomaten-Alias zu erstellen	Schreiben	statemachine*		
				states:StateMachineQualifier	
DeleteActivity	Gewährt die Berechtigung zum Löschen einer Aktivität	Write	activity*		
DeleteStateMachine	Gewährt die Berechtigung zum Löschen eines Zustandsautomaten	Schreiben	statemachine*		
DeleteStateMachineAlias	Gewährt die Berechtigung, einen Zustandsautomaten-Alias zu löschen	Schreiben	statemachine*		
				states:StateMachineQualifier	
DeleteStateMachineVersion	Gewährt die Berechtigung, eine Zustandsautomaten-Version zu löschen	Schreiben	statemachine*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				states:StateMachineQualifier	
DescribeActivity	Gewährt die Berechtigung zum Beschreiben einer Aktivität	Lesen	activity*		
DescribeExecution	Gewährt die Berechtigung zum Beschreiben einer Ausführung	Lesen	execution*		
			express*		
DescribeMapRun	Gewährt die Berechtigung zum Beschreiben einer Zuordnungsausführung	Lesen	maprun*		
DescribeStateMachine	Gewährt die Berechtigung zum Beschreiben eines Zustandsautomaten	Lesen	statemachine*		
				states:StateMachineQualifier	
DescribeStateMachineAlias	Gewährt die Berechtigung, einen Zustandsautomaten-Alias zu beschreiben	Lesen	statemachine*		
				states:StateMachineQualifier	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeStateMachineForExecution	Gewährt die Berechtigung zum Beschreiben des Zustandsautomaten für eine Ausführung	Lesen	execution*		
GetActivityTask	Gewährt die Berechtigung, eine Aufgabe (mit dem angegebenen Aktivitäts-ARN) abzurufen, die für die Ausführung durch einen laufenden Zustandsautomaten geplant wurde	Write	activity*		
GetExecutionHistory	Gewährt die Berechtigung, den Verlauf der angegebenen Ausführung als Liste von Ereignissen zurückzugeben	Lesen	execution*		
InvokeHTTPEndpoint [nur Berechtigung]	Gewährt die Berechtigung, den HTTP-Task-Status aufzurufen	Schreiben			
ListActivities	Gewährt die Berechtigung zum Auflisten der vorhandenen Aktivitäten	List			
ListExecutions	Gewährt die Berechtigung zum Auflisten der Ausführungen eines Zustandsautomaten	Auflisten	maprun*		
			statemachine*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				states:StateMachineQualifier	
ListMapRuns	Gewährt die Berechtigung zum Auflisten der Zuordnungsausführungen einer Ausführung	Auflisten	execution*		
ListStateMachineAliases	Gewährt die Berechtigung, die Aliasse eines Zustandsautomaten aufzulisten	Auflisten	statemachine*		
				states:StateMachineQualifier	
ListStateMachineVersions	Gewährt die Berechtigung, die Versionen eines Zustandsautomaten aufzulisten	Auflisten	statemachine*		
ListStateMachines	Gewährt die Berechtigung zum Auflisten der vorhandenen Zustandsautomaten	Auflisten			
ListTagsForResource	Erteilt die Berechtigung, Tags für eine AWS Step Functions Functions-Ressource aufzulisten	Auflisten	activity		
			statemachine		
PublishStateMachineVersion	Gewährt die Berechtigung, eine Zustandsautomaten-Version zu veröffentlichen	Schreiben	statemachine*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RedriveExecution	Gewährt die Berechtigung zum Neuauffahren einer Ausführung	Schreiben	execution*		
RevealSecrets [nur Berechtigung]	Gewährt die Berechtigung, vertrauliche Daten aus einer Ausführung preiszugeben	Lesen			
SendTaskFailure	Gewährt die Berechtigung, zu melden, dass die durch das taskToken identifizierte Aufgabe fehlgeschlagen ist	Write			
SendTaskHeartbeat	Gewährt die Berechtigung, zu melden, dass die durch das angegebene taskToken repräsentierte Aufgabe immer noch Fortschritte macht	Write			
SendTaskSuccess	Gewährt die Berechtigung, zu melden, dass die durch das taskToken identifizierte Aufgabe erfolgreich abgeschlossen wurde	Write			
StartExecution	Gewährt die Berechtigung, die Ausführung eines Zustandsautomaten zu starten	Write	statemachine*		
				states:StateMachineQualifier	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartSyncExecution	Gewährt die Berechtigung, die Ausführung eines Synchronous-Express-Zustandsautomaten zu starten	Write	statemachine*		
				states:StateMachineQualifier	
StopExecution	Gewährt die Berechtigung zum Stoppen einer Ausführung	Schreiben	execution*		
TagResource	Erteilt die Berechtigung, eine AWS Step Functions Functions-Ressource zu taggen	Tagging	activity		
			statemachine		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
TestState	Gewährt die Berechtigung zum Testen eine Zustandsautomaten-Definition	Schreiben			states:RevealSecrets
UntagResource	Erteilt die Berechtigung, ein Tag aus einer AWS Step Functions Functions-Ressource zu entfernen	Tagging	activity		
			statemachine		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateMapRun	Gewährt die Berechtigung zum Aktualisieren einer Zuordnungsausführung	Schreiben	maprun*		
UpdateStateMachine	Gewährt die Berechtigung zum Aktualisieren eines Zustandsautomaten	Schreiben	statemachine*		iam:PassRole states:PublishStateMachineVersion
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateStateMachineAlias	Gewährt die Berechtigung, einen Zustandsautomaten-Alias zu aktualisieren	Schreiben	statemachine*		
				states:StateMachineQualifier	
ValidateStateMachineDefinition	Erteilt die Berechtigung zur Validierung einer State-Machine-Definition	Lesen			

Von AWS Step Functions definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
activity	`arn:${Partition}:states:${Region}:${Account}:activity:${ActivityName}`	aws:ResourceTag/${TagKey}
execution	`arn:${Partition}:states:${Region}:${Account}:execution:${StateMachineName}:${ExecutionId}`	aws:ResourceTag/${TagKey}
express	`arn:${Partition}:states:${Region}:${Account}:express:${StateMachineName}:${ExecutionId}:${ExpressId}`	
statemachine	`arn:${Partition}:states:${Region}:${Account}:stateMachine:${StateMachineName}`	aws:ResourceTag/${TagKey}
statemachineversion	`arn:${Partition}:states:${Region}:${Account}:stateMachine:${StateMachineName}:${StateMachineVersionId}`	
statemachinealias	`arn:${Partition}:states:${Region}:${Account}:stateMachine:${StateMachineName}:${StateMachineAliasName}`	
maprun	`arn:${Partition}:states:${Region}:${Account}:mapRun:${StateMachineName}/${MapRunLabel}:${MapRunId}`	

Ressourcentypen	ARN	Bedingungsschlüssel
labelled execution	`arn:${Partition}:states:${Region}:${Account}:execution:${StateMachineName}/${MapRunLabel}:${ExecutionId}`	
labelled express	`arn:${Partition}:states:${Region}:${Account}:express:${StateMachineName}/${MapRunLabel}:${ExecutionId}:${ExpressId}`	

Bedingungsschlüssel für AWS Step Functions

AWS Step Functions definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wertepaaren, die in der Anforderung zulässig sind	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paar einer Ressource	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach Liste von Tag-Schlüsseln, die in der Anforderung zulässig sind	ArrayOfString
states:HTTPEndpoint	Filtert den Zugriff nach dem Endpunkt, den der HTTP-Task-Status in der Anfrage zulässt	String

Bedingungsschlüssel	Beschreibung	Typ
states:HTTPMethod	Filtert den Zugriff nach der Methode, die der HTTP-Task-Status in der Anfrage zulässt	String
states:StateMachineQualifier	Filtert den Zugriff nach dem Qualifizierer eines Zustandsautomaten-ARN	String

Aktionen, Ressourcen und Zustandsschlüssel für AWS Storage Gateway

AWS Storage Gateway (Servicepräfix: `storagegateway`) bietet die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Storage Gateway definierte Aktionen
- Von AWS Storage Gateway definierte Ressourcentypen
- Bedingungsschlüssel für AWS Storage Gateway

Von AWS Storage Gateway definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ActivateGateway	Gewährt die Berechtigung, das Gateway zu aktivieren, das Sie zuvor auf Ihrem Host bereitgestellt haben	Write		aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys	
AddCache	Gewährt die Berechtigung zum Konfigurieren einer oder mehrerer lokaler Gateway-Festplatten als Cache für ein Cached-Volume-Gateway	Write	gateway*		
AddTagsToResource	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Tags zur angegebenen Ressource	Markieren	gateway		
			share		
			tape		
			volume		
				aws:RequestTag/${TagKey} aws:TagKeys	
AddUploadBuffer	Gewährt die Berechtigung zum Konfigurieren einer oder mehrerer lokaler Gateway-Festplatten als Upload-Puffer für ein bestimmtes Gateway	Write	gateway*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddWorkingStorage	Gewährt die Berechtigung, eine oder mehrere lokale Gateway-Festplatten als Arbeitsspeicher für ein Gateway zu konfigurieren	Write	gateway*		
AssignTapePool	Gewährt die Berechtigung, ein Band in den angegebenen Zielpool zu verschieben	Write	tape* tapepool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Associate FileSystem	Gewährt die Berechtigung, ein Amazon FSx-Dateisystem mit dem Amazon FSx-Datei-Gateway zu verknüpfen	Write	gateway*		ds:DescribeDirectories ec2:DescribeNetworkInterfaces fsx:DescribeFileSystems iam:CreateServiceLinkedRole logs:CreateLogDelivery logs:GetLogDelivery logs:ListLogDeliveries logs:UpdateLogDelivery

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
AttachVolume	Bei dieser Produktion wird ein Volume mit einer iSCSI-Verbindung verbunden und dann an das angegebene Gateway angefügt.	Write	gateway* volume*		
BypassGovernanceRetention	Gewährt die Berechtigung, die Governance-Aufbewahrungssperre für einen Pool zu umgehen	Write	tapepool*		
CancelArchival	Gewährt die Berechtigung, die Archivierung eines virtuellen Bands auf dem virtuellen Bandregal (VTS) abzubrechen, nachdem der Archivierungsprozess eingeleitet wird	Write	gateway* tape*		
CancelRetrieval	Gewährt die Berechtigung, den Abruf eines virtuellen Bands vom virtuellen Bandregal (VTS) zu einem Gateway abzubrechen, nachdem der Abrufvorgang initiiert wird	Write	gateway* tape*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCachediSCSIVolume	Gewährt die Berechtigung zum Erstellen eines Cached-Volumes auf einem angegebenen Cached-Gateway. Diese Produktion wird nur für die Gateway-Cached-Volume-Architektur unterstützt.	Write	gateway*		
			volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNFSFileShare	Gewährt die Berechtigung zum Erstellen einer NFS-Dateifreigabe auf einem vorhandenen Datei-Gateway	Write	gateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSMBFileShare	Gewährt die Berechtigung zum Erstellen einer SMB-Dateifreigabe auf einem vorhandenen Datei-Gateway	Write	gateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshot	Gewährt die Berechtigung, einen Snapshot eines Volumes zu initiieren	Write	volume*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshotFromVolumeRecoveryPoint	Gewährt die Berechtigung, einen Snapshot eines Gateways aus einem Volume-Wiederherstellungspunkt	Write	volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStorediSCSIVolume	Gewährt die Berechtigung zum Erstellen eines Volumes auf einem bestimmten Gateway	Write	gateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTapePool	Gewährt die Berechtigung zum Erstellen einer Tabelle.	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTapeWithBarcode	Gewährt die Erlaubnis, ein virtuelles Band mit Ihrem eigenen Barcode zu erstellen	Write	gateway*		
			tapepool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTapes	Gewährt die Berechtigung zum Erstellen eines oder mehrerer virtueller Bänder. Sie schreiben Daten auf die virtuellen Bänder und archivieren dann die Bänder.	Write	gateway*		
			tapepool*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAutomaticTapeCreationPolicy	Gewährt die Berechtigung zum Löschen der Richtlinie zur automatischen Bandersterstellung, die in einem Gateway-VTL konfiguriert ist	Write	gateway*		
DeleteBandwidthRateLimit	Gewährt die Berechtigung zum Löschen der Bandbreitenratengrenzen eines Gateways	Write	gateway*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteChapCredentials	Diese Produktion löscht Challenge-Handshake Authentication Protocol (CHAP)-Anmeldeinformationen für ein bestimmtes iSCSI-Ziel und Initiator-Paar.	Write	target*		
DeleteFileShare	Gewährt die Berechtigung zum Löschen einer Dateifreigabe von einem Datei-Gateway	Write	share*		
DeleteGateway	Gewährt die Berechtigung zum Löschen eines Gateways	Write	gateway*		
DeleteSnapshotSchedule	Gewährt die Berechtigung zum Löschen eines Snapshots eines Volumes	Write	volume*		
DeleteTape	Gewährt die Berechtigung zum Löschen des angegebenen virtuellen Bandes	Write	gateway*		
			tape*		
DeleteTapeArchive	Gewährt die Berechtigung, das angegebene virtuelle Band aus dem virtuellen Bandregal (VTS) zu löschen	Write			
DeleteTapePool	Gewährt die Berechtigung zum Löschen des angegebenen Band-Pool	Write	tapepool*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteVolume	Gewährt die Berechtigung zum Löschen des angegebenen Gateway-Volumes, das Sie zuvor mit der CreateCacheDiscsiVolume- oder CreateStoreDiscsiVolume-API erstellt haben	Write	volume*		
DescribeAvailabilityMonitorTest	Gewährt die Berechtigung zum Abrufen der Informationen über den neuesten Hochverfügbarkeitsüberwachungstest, der am Gateway durchgeführt wurde	Read	gateway*		
DescribeBandwidthRateLimit	Gewährt die Berechtigung zum Abrufen der Bandbreitenratengrenzen eines Gateways	Read	gateway*		
DescribeBandwidthRateLimitSchedule	Gewährt die Berechtigung, den Zeitplan für das Bandbreitenlimit eines Gateways zu erhalten	Read	gateway*		
DescribeCache	Gewährt die Berechtigung, Informationen über den Cache eines Gateways zu erhalten. Diese Produktion wird nur für die Gateway-Cached-Volume-Architektur unterstützt.	Read	gateway*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeCachediSCSIVolumes	Gewährt die Berechtigung zum Abrufen einer Beschreibung der in der Anfrage angegebenen Gateway-Volumes. Diese Produktion wird nur für die Gateway-Cached-Volume-Architektur unterstützt.	Read	volume*		
DescribeChapCredentials	Gewährt die Berechtigung zum Abrufen eines Arrays von CHALENGE-Handshake Authentication Protocol (CHAP) für ein bestimmtes iSCSI-Ziel, eines für jedes Zielinitiatorenpaar	Read	target*		
DescribeFileSystemAssociations	Gewährt die Berechtigung zum Abrufen einer Beschreibung für eine oder mehrere Dateisystemmappingen	Read	fs-association*		
DescribeGatewayInformation	Gewährt die Berechtigung zum Abrufen von Metadaten über ein Gateway wie seinen Namen, seine Netzwerkschnittstellen, die konfigurierte Zeitzone und den Status (ob das Gateway läuft oder nicht)	Read	gateway*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeMaintenanceStartTime	Gewährt die Erlaubnis, die wöchentliche Wartungsstartzeit Ihres Gateways zu erhalten, einschließlich Tag und Uhrzeit der Woche	Read	gateway*		
DescribeNFSFileShares	Gewährt die Berechtigung zum Abrufen einer Beschreibung für eine oder mehrere Dateifreigaben von einem File Gateway	Read	share*		
DescribeSMBFileShares	Gewährt die Berechtigung zum Abrufen einer Beschreibung für eine oder mehrere Dateifreigaben von einem File Gateway	Read	share*		
DescribeSMBSettings	Bei dieser Produktion wird eine Beschreibung der Server Message Block (SMB)-Dateifreigabe-Einstellungen aus einem Datei-Gateway abgerufen.	Read	gateway*		
DescribeSnapshotSchedule	Gewährt die Berechtigung, den Snapshot-Zeitplan für das angegebene Gateway-Volume	Read	volume*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeStorediSCSIVolumes	Gewährt die Berechtigung zum Abrufen einer Beschreibung der in der Anfrage angegebenen Gateway-Volumes.	Read	volume*		
DescribeTapeArchives	Gewährt die Erlaubnis, eine Beschreibung bestimmter virtueller Bänder im virtuellen Band-Shelf (VTS) zu erhalten	Read			
DescribeTapeRecoveryPoints	Gibt eine Liste der Wiederherstellungspunkte der virtuellen Bänder zurück, die für die angegebene Gateway-VTL verfügbar sind.	Read	gateway*		
DescribeTapes	Gibt eine Beschreibung des angegebenen Amazon-Ressourcennamens (ARN) der virtuellen Bänder zurück.	Read	gateway*		
DescribeUploadBuffer	Gewährt die Berechtigung, Informationen über den Upload-Puffer eines Gateways zu erhalten	Read	gateway*		
DescribeVTLDevices	Gewährt die Berechtigung zum Abrufen einer der virtuellen Bandbibliothek (Virtual Tape Library (VTL))-Geräte für das angegebene Gateway	Read	gateway*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeWorkingStorage	Gewährt die Berechtigung zum Abrufen von Informationen über den Arbeitsspeicher eines Gateways	Read	gateway*		
DetachVolume	Gewährt die Berechtigung, ein Volume von einer iSCSI-Verbindung zu trennen, und trennt dann das Volume vom angegebenen Gateway	Write	volume*		
DisableGateway	Gewährt die Berechtigung zum Deaktivieren eines Gateways, wenn das Gateway nicht mehr funktioniert	Write	gateway*		
DisassociateFileSystem	Gewährt die Berechtigung, ein Amazon FSx-Dateisystem von einem Amazon FSx-Datei-Gateway zu trennen	Write	fs-association*		
JoinDomain	Gewährt die Berechtigung zum Beitritt zu einer Active Directory-Domain	Schreiben	gateway*		
ListAutomaticTapeCreationPolicies	Gewährt die Berechtigung zum Auflisten der Richtlinie zur automatischen Banderstellung, die für das angegebene Gateway-VTL oder alle Gateway-VTLs Ihres AWS-Kontos konfiguriert sind	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListFileShares	Gewährt die Berechtigung zum Abrufen einer Liste der Dateifreigaben für ein bestimmtes File Gateway oder die Liste der Dateifreigaben, die zu Ihrem AWS-Konto gehören	Auflisten			
ListFileSystemAssociations	Gewährt die Berechtigung zum Abrufen einer Liste der Dateisystemmappingen für das angegebene Gateway	List			
ListGateways	Gewährt die Berechtigung zum Auflisten von Gateways, die einem AWS-Konto in einer in der Anfrage angegebenen Region gehören. Die zurückgegebene Liste wird nach Amazon-Ressourcenname (ARN) des Gateways sortiert.	List			
ListLocalDisks	Gewährt die Berechtigung, eine Liste der lokalen Festplatten des Gateways zu erhalten	List	gateway*		
ListTagsForResource	Gewährt die Berechtigung, die Tags zu erhalten, die der angegebenen Ressource hinzugefügt wurden	List	gateway		
			share		
			tape		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			volume		
ListTapePools	Gewährt die Berechtigung, Band-Pools aufzulisten, die Ihrem AWS-Konto gehören	List			
ListTapes	Gewährt die Berechtigung zum Auflisten virtueller Bänder in Ihrer virtuellen Bandbibliothek (VTL) und Ihrem virtuellen Bandregal (VTS)	List			
ListVolumeInitiators	Gewährt die Berechtigung zum Auflisten von iSCSI-Initiatoren, die mit einem Volume verbunden sind	List	volume*		
ListVolumeRecoveryPoints	Gewährt die Berechtigung zum Auflisten der Wiederherstellungspunkte für ein bestimmtes Gateway	List	gateway*		
ListVolumes	Gewährt die Berechtigung zum Auflisten der iSCSI-gespeicherten Volumes eines Gateways	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
NotifyWhenUploaded	Gewährt die Berechtigung, Ihnen eine Benachrichtigung über CloudWatch Events zu senden, wenn alle in Ihre NFS-Dateifreigabe geschriebenen Dateien auf Amazon S3 hochgeladen wurden	Write	share*		
RefreshCache	Gewährt die Berechtigung, den Cache für die angegebene Dateifreigabe zu aktualisieren	Write	share*		
RemoveTagsFromResource	Gewährt die Berechtigung zum Entfernen eines oder mehrerer Tags aus der angegebenen Ressource	Markieren	gateway		
			share		
			tape		
			volume		
				aws:TagKeys	
ResetCache	Gewährt die Berechtigung zum Zurücksetzen aller Cache-Datenträger, die auf einen Fehler gestoßen sind, und stellt die Datenträger für die Neukonfiguration als Cache-Speicher zur Verfügung	Write	gateway*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RetrieveTapeArchive	Gewährt die Berechtigung zum Abrufen eines archivierten virtuellen Bands vom virtuellen Bandregal (VTS) zu einem Gateway-VTL	Write	gateway* tape*		
RetrieveTapeRecoveryPoint	Gewährt die Berechtigung zum Abrufen des Wiederherstellungspunkts für das angegebene virtuelle Band	Write	gateway* tape*		
SetLocalConsolePassword	Gewährt die Berechtigung zum Festlegen des Kennworts für Ihre lokale VM-Konsole	Write	gateway*		
SetSMBGuestPassword	Gewährt die Berechtigung zum Festlegen des Kennworts für SMB Guest-Benutzer	Write	gateway*		
ShutdownGateway	Gewährt die Berechtigung zum Herunterfahren eines Gateways	Write	gateway*		
StartAvailabilityMonitorTest	Gewährt die Berechtigung zum Starten eines Tests, der überprüft, ob das angegebene Gateway für die Hochverfügbarkeitsüberwachung in Ihrer Hostumgebung konfiguriert ist	Write	gateway*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartGateway	Gewährt die Berechtigung zum Starten eines Gateways, das Sie zuvor heruntergefahren haben	Write	gateway*		
UpdateAutomaticTapeCreationPolicy	Gewährt die Berechtigung zum Aktualisieren der Richtlinie zur automatischen Banderstellung, die für ein Gateway-VTL konfiguriert ist	Write	gateway* tapepool*		
UpdateBandwidthRateLimit	Gewährt die Berechtigung zur Aktualisierung der Bandbreitenratengrenzen eines Gateways	Write	gateway*		
UpdateBandwidthRateLimitSchedule	Gewährt die Berechtigung zur Aktualisierung des Zeitplans für das Bandbreitenlimit eines Gateways	Write	gateway*		
UpdateChapCredentials	Gewährt die Berechtigung zum Aktualisieren der Anmeldeinformationen für das Challenge-Handshake Authentication Protocol (CHAP) für ein bestimmtes iSCSI-Ziel	Write	target*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateFileSystemAssociation	Gewährt die Berechtigung zum Aktualisieren einer Dateisystemmapping	Write	fs-association*		logs:CreateLogDelivery logs:DeleteLogDelivery logs:GetLogDelivery logs:ListLogDeliveries logs:UpdateLogDelivery
UpdateGatewayInformation	Gewährt die Berechtigung zum Aktualisieren der Metadaten eines Gateways, einschließlich des Namens und der Zeitzone des Gateways	Write	gateway*		
UpdateGatewaySoftwareNow	Gewährt die Berechtigung zum Aktualisieren der virtuellen Gateway-Maschine (VM)-Software	Write	gateway*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateMaintenanceStartTime	Gewährt die Berechtigung, die wöchentlichen Wartungsstartzeitinformationen eines Gateways zu aktualisieren, einschließlich Tag und Uhrzeit der Woche. Die Wartungszeit ist die Zeit in der Zeitzone Ihres Gateways.	Write	gateway*		
UpdateNFSFileShare	Gewährt die Berechtigung zum Aktualisieren einer NFS-Dateifreigabe	Write	share*		
UpdateSMBFileShare	Gewährt die Berechtigung zum Aktualisieren einer SMB-Dateifreigabe	Write	share*		
UpdateSMBFileShareVisibility	Gewährt die Berechtigung zum Aktualisieren, ob die Freigaben auf einem Gateway in einer Netzansicht oder einer Suchliste sichtbar sind	Schreiben	gateway*		
UpdateSMBLocalGroups	Erteilt die Berechtigung zum Aktualisieren der Liste der Active Directory-Benutzer und -Gruppen, die über spezielle Berechtigungen für SMB-Dateifreigaben im Gateway verfügen	Schreiben	gateway*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateSMBSecurityStrategy	Gewährt die Berechtigung zur Aktualisierung der SMB-Sicherheitsstrategie für ein Datei-Gateway	Write	gateway*		
UpdateSnapshotSchedule	Gewährt die Berechtigung zum Aktualisieren eines für ein Gateway-Volume konfigurierten Snapshot-Zeitplans	Write	volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateVTLDeviceType	Gewährt die Berechtigung, den Typ des mittleren Mediums in einem Gateway-VTL zu aktualisieren	Schreiben	device*		

Von AWS Storage Gateway definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressource ntypen	ARN	Bedingungsschlüssel
device	arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}/device/${Vtldevice}	
fs-association	arn:${Partition}:storagegateway:${Region}:${Account}:fs-association/${FsaId}	aws:ResourceTag/${TagKey}
gateway	arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}	aws:ResourceTag/${TagKey}
share	arn:${Partition}:storagegateway:${Region}:${Account}:share/${ShareId}	aws:ResourceTag/${TagKey}
tape	arn:${Partition}:storagegateway:${Region}:${Account}:tape/${TapeBarcode}	aws:ResourceTag/${TagKey}
tapepool	arn:${Partition}:storagegateway:${Region}:${Account}:tapepool/${PoolId}	aws:ResourceTag/${TagKey}
target	arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}/target/${IscsiTarget}	
volume	arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}/volume/${VolumeId}	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Storage Gateway

AWS Storage Gateway definiert die folgenden Bedingungsschlüssel, die in einem `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den zulässigen Werten für jeden der Tags	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Tag-Wert, der der Ressource zugeordnet ist	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach dem Vorhandensein verbindlicher Tags in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für die AWS -Lieferkette

AWS Supply Chain (Dienstpräfix:`scn`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Durch die AWS -Lieferkette definierte Aktionen
- Durch eine AWS -Lieferkette definierte Ressourcentypen
- Bedingungsschlüssel für eine AWS -Lieferkette

Durch die AWS -Lieferkette definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssignAdminPermissionsToUser	Erteilt einem Verbundbenutzer die Berechtigung, AWS Supply-Chain-Administratorrechte hinzuzufügen	Schreiben	instance*		
CreateBillOfMaterialsImportJob	Erteilt die Berechtigung zum Erstellen einer Datei BillOfMaterialsImportJob , die eine CSV-Datei mit Datensätzen importiert BillOfMaterials	Schreiben	instance*		
CreateInstance	Erteilt die Erlaubnis, eine neue AWS Supply-Chain-Instanz zu erstellen	Schreiben	instance*		
CreateSSOApplication	Erteilt die Erlaubnis, eine IAM Identity Center-Anwendung für eine AWS Supply Chain-Instanz zu erstellen	Schreiben	instance*		
DeleteInstance	Erteilt die Berechtigung zum Löschen einer AWS Supply Chain-Instanz	Schreiben	instance*		
DeleteSSOApplication	Erteilt die Berechtigung zum Löschen der IAM Identity Center-Anwendung der AWS Supply Chain-Instanz	Schreiben	instance*		
DescribeInstance	Erteilt die Berechtigung, Details einer AWS Supply-Chain-Instanz einzusehen	Lesen	instance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetBillOfMaterialsImportJob	Erteilt die Berechtigung zum Anzeigen des Status und der Details einer BillOfMaterialsImportJob	Lesen	bill-of-materials-import-job*		
ListAdminUsers	Erteilt die Berechtigung, AWS Supply-Chain-Administratoren einer Instanz aufzulisten	Auflisten	instance*		
ListInstances	Erteilt die Berechtigung zum Anzeigen der AWS Supply-Chain-Instanzen, die mit einem verknüpft sind AWS-Konto	Auflisten	instance*		
ListTagsForResource	Erteilt die Berechtigung, Tags für eine AWS Supply-Chain-Instanz aufzulisten	Auflisten	instance*		
RemoveAdminPermissionsForUser	Erteilt die Berechtigung, einem Verbundbenutzer die AWS Supply-Chain-Administratorberechtigung zu entziehen	Schreiben	instance*		
SendDataIntegrationEvent	Erteilt die Erlaubnis, eine zu erstellen DataIntegrationEvent , die Daten in Echtzeit aufnimmt	Schreiben	instance*		
TagResource	Erteilt die Erlaubnis, eine AWS Supply-Chain-Instanz zu taggen	Tagging	instance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Erteilt die Berechtigung zum Entfernen eines Tags aus einer AWS Supply-Chain-Instanz	Tagging	instance*		
				aws:TagKeys	
UpdateInstance	Erteilt die Erlaubnis, eine AWS Supply-Chain-Instanz zu aktualisieren	Schreiben	instance*		

Durch eine AWS -Lieferkette definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
instance	`arn:${Partition}:scn:${Region}:${Account}:instance/${InstanceId}`	

Ressourcentypen	ARN	Bedingungsschlüssel
bill-of-materials-import-job	`arn:${Partition}:scn:${Region}:${Account}:instance/${InstanceId}/bill-of-materials-import-job/${JobId}`	

Bedingungsschlüssel für eine AWS -Lieferkette

AWS Supply Chain definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff mithilfe von Tag-Schlüssel-Wert-Paaren in der Anforderung	String
aws:ResourceTag/${TagKey}	Filtert Aktionen mithilfe von Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert den Zugriff mithilfe von Tag-Schlüsseln in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Support

AWS Support (Servicepräfix: `support`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Support definierte Aktionen
- Von AWS Support definierte Ressourcentypen
- Bedingungsschlüssel für AWS Support

Von AWS Support definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

> **Note**
>
> AWS Support bietet die Möglichkeit, auf Fälle zuzugreifen, sie zu ändern und zu lösen sowie Trusted-Advisor-Aktionen zu verwenden. Wenn Sie die Support-API zum Aufrufen von auf Trusted Advisor bezogenen Aktionen verwenden, schränkt keine der „trustedadvisor: *“-Aktionen Ihren Zugriff ein. Die „trustedadvisor:*“-Aktionen gelten nur für Trusted Advisor in der AWS Management Console.

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddAttachmentsToSet	Gewährt die Berechtigung, einem AWS Support-Fall einen oder mehrere Anhänge hinzuzufügen	Schreiben			
AddCommunicationToCase	Gewährt die Berechtigung, einem AWS Support-Fall eine Kundenmitteilung hinzuzufügen	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCase	Gewährt die Berechtigung, einen neuen AWS Support-Fall zu erstellen	Schreiben			
DescribeAttachment	Gewährt die Berechtigung, Anhangsdetails zu beschreiben	Lesen			
DescribeCaseAttributes	Gewährt die Berechtigung, sekundären Services das Lesen von AWS Support-Fallattributen zu gestatten. Dies ist eine intern verwaltete Funktion.	Lesen			
DescribeCases	Gewährt die Berechtigung, AWS Support-Fälle aufzulisten, die den angegebenen Eingaben entsprechen	Lesen			
DescribeCommunication	Gewährt die Berechtigung zum Abrufen einer einzelnen Mitteilung und Anhängen für einen einzelnen AWS Support-Fall	Lesen			
DescribeCommunications	Gewährt die Berechtigung, die Mitteilungen und Anhänge für einen oder mehrere AWS Support-Fälle aufzulisten	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeCreateCaseOptions	Gewährt die Berechtigung, die verfügbaren Optionen für die Erstellung eines Support-Falls zu beschreiben	Lesen			
DescribeIssueTypes	Gewährt die Berechtigung, Problemtypen für AWS Support-Fälle zurückzugeben	Lesen			
DescribeServices	Gewährt die Berechtigung, AWS-Services und die für jeden Service zutreffenden Kategorien aufzulisten	Lesen			
DescribeSeverityLevels	Gewährt die Berechtigung, Schweregrade aufzulisten, die einem AWS Support-Fall zugewiesen werden können	Lesen			
DescribeSupportLevel	Gewährt die Berechtigung, die Support-Stufe für eine AWS-Konto-Kennung zurückzugeben	Lesen			
DescribeSupportedLanguages	Gewährt die Berechtigung, die verfügbaren Support-Sprachen für einen Kategoriecode, Servicecode und Problemtyp zu beschreiben	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeTrustedAdvisorCheckRefreshStatuses	Gewährt die Berechtigung, den Status einer Trusted-Advisor-Aktualisierungsprüfung basierend auf einer Liste von Prüfungskennungen abzurufen	Lesen			
DescribeTrustedAdvisorCheckResult	Gewährt die Berechtigung, das Ergebnis der Trusted-Advisor-Prüfung mit der angegebenen Prüfungskennung abzurufen	Lesen			
DescribeTrustedAdvisorCheckSummaries	Gewährt die Berechtigung, die Zusammenfassungen der Ergebnisse der Trusted-Advisor-Prüfungen mit den angegebenen Prüfungskennungen abzurufen	Lesen			
DescribeTrustedAdvisorChecks	Gewährt die Berechtigung, eine Liste aller verfügbaren Trusted-Advisor-Prüfungen abzurufen, einschließlich Name, Kennung, Kategorie und Beschreibung	Lesen			
InitiateCallForCase	Gewährt die Berechtigung, einen Anruf im AWS Support-Center zu starten Dies ist eine intern verwaltete Funktion.	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
InitiateChatForCase	Gewährt die Berechtigung, einen Chat im AWS Support-Center zu starten. Dies ist eine intern verwaltete Funktion.	Schreiben			
PutCaseAttributes	Gewährt die Berechtigung, sekundären Services das Hinzufügen von Attributen zu AWS Support-Fällen zu gestatten. Dies ist eine intern verwaltete Funktion.	Schreiben			
RateCaseCommunication	Gewährt die Berechtigung, die Kommunikation zu einem AWS Support-Fall zu bewerten	Schreiben			
RefreshTrustedAdvisorCheck	Gewährt die Berechtigung, eine Aktualisierung der Trusted-Advisor-Prüfung mit der angegebenen Prüfungskennung anzufordern	Schreiben			
ResolveCase	Gewährt die Berechtigung, einen AWS Support-Fall zu lösen	Schreiben			
SearchForCases	Gewährt die Berechtigung, eine Liste von AWS Support-Fällen zurückzugeben, die den jeweiligen Eingaben entsprechen	Lesen			

Von AWS Support definierte Ressourcentypen

AWS Support unterstützt nicht die Angabe eines Ressourcen-ARN im Element `Resource` einer IAM-Richtlinienanweisung. Um den Zugriff auf AWS Support zuzulassen, geben Sie in Ihrer Richtlinie `"Resource": "*"` an.

Bedingungsschlüssel für AWS Support

Support besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für die AWS Support-App in Slack

Die AWS Support-App in Slack (Service-Präfix: `supportapp`) stellt die folgenden service-spezifischen Ressourcen, Aktionen und Bedingungsschlüssel für die Verwendung in IAM-Berechtigungs-Richtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von der AWS Support-App in Slack definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den

Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSlackChannelConfiguration	Gewährt die Berechtigung zum Erstellen einer Slack-Channel-Konfiguration für Ihr Konto	Schreiben			
DeleteAccountAlias	Gewährt die Berechtigung zum Löschen eines Alias aus Ihrem Konto	Schreiben			
DeleteSlackChannelConfiguration	Gewährt die Berechtigung zum Löschen einer Slack-Channel-Konfiguration aus Ihrem Konto	Schreiben			
DeleteSlackWorkspaceConfiguration	Gewährt die Berechtigung zum Löschen einer Slack-Workspace-Konfiguration aus Ihrem Konto	Schreiben			
DescribeSlackChannels [nur Berechtigung]	Gewährt die Berechtigung, alle öffentlichen Slack-Kanäle in einem Workspace aufzulisten, die die AWS Support-App eingeladen haben	Lesen			
GetAccountAlias	Gewährt die Berechtigung zum Abrufen eines Alias für Ihr Konto	Lesen			
GetSlackOauthParameters [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Parametern für den OAuth-Code von Slack, den die AWS Support-	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	App verwendet, um den Workspace zu autorisieren				
ListSlackChannelConfigurations	Gewährt die Berechtigung zum Auflisten aller Slack-Channel-Konfigurationen für Ihr Konto	Lesen			
ListSlackWorkspaceConfigurations	Gewährt die Berechtigung zum Auflisten aller Slack-Workspace-Konfigurationen für Ihr Konto	Lesen			
PutAccountAlias	Gewährt die Berechtigung zum Erstellen oder Aktualisieren eines Alias für Ihr Konto	Schreiben			
RedeemSlackOauthCode [nur Berechtigung]	Gewährt die Berechtigung zum Einlösen des Slack-OAuth-Codes, den die AWS Support-App zum Autorisieren des Workspace verwendet	Schreiben			
RegisterSlackWorkspaceForOrganization	Gewährt die Berechtigung zum Registrieren eines Slack-Workspace für ein AWS-Konto, das Teil einer Organisation ist	Schreiben			
UpdateSlackChannelConfiguration	Gewährt die Berechtigung zum Aktualisieren einer Slack-Channel-Konfiguration für Ihr Konto	Schreiben			

Von AWS Support-App in Slack definierte Ressourcentypen

Die AWS Support-App in Slack unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf die AWS Support-App in Slack zuzulassen, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Support-App in Slack

Support App hat keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Support Plans

AWS Support Plans (Servicepräfix: `supportplans`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Support Plans (Plänen) definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSupportPlanSchedule [nur Berechtigung]	Gewährt die Berechtigung zur Erstellung von Support-Plan-Zeitplänen für dieses AWS-Konto	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetSupportPlan [nur Berechtigung]	Erteilt die Berechtigung zum Anzeigen von Details zum aktuellen Support-Plan für diesen AWS-Konto	Lesen			
GetSupportPlanUpdateStatus [nur Berechtigung]	Erteilt die Berechtigung zum Anzeigen von Details zum Status einer Anfrage zum Aktualisieren eines Supportplans	Lesen			
StartSupportPlanUpdate [nur Berechtigung]	Erteilt die Berechtigung zum Aktualisieren des Supportplans dafür dieses AWS-Konto	Schreiben			

Von AWS Support Plans definierte Ressourcentypen

AWS Support Plans unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf AWS Support Plans zu ermöglichen, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Support Plans

Support Plans hat keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS-Nachhaltigkeit

AWS-Nachhaltigkeit (Servicepräfix: `sustainability`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Aktionen definiert durch AWS-Nachhaltigkeit
- Von AWS-Nachhaltigkeit definierte Ressourcentypen
- Bedingungsschlüssel für AWS-Nachhaltigkeit

Aktionen definiert durch AWS-Nachhaltigkeit

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetCarbonFootprintSummary	Gewährt die Berechtigung zum Anzeigen des CO2-Fußabdruck-Tools	Lesen			

Von AWS-Nachhaltigkeit definierte Ressourcentypen

AWS-Nachhaltigkeit unterstützt die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf AWS-Nachhaltigkeit zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS-Nachhaltigkeit

Nachhaltigkeit umfasst keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Systems Manager

AWS Systems Manager (Servicepräfix: `ssm`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Systems Manager definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddTagsToResource	Gewährt die Berechtigung zum Hinzufügen oder Überschreiben eines oder mehrerer Tags für eine angegebene AWS Ressource	Tagging	association		
			automation-execution		
			document		
			instance		
			maintenancewindow		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			managed-instance		
			opsitem		
			opsmetadata		
			parameter		
			patchbaseline		
			task		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
AssociateOpsItemRelatedItem	Gewährt die Berechtigung zum Zuordnen RelatedItem zu einem OpsItem	Schreiben	opsitem*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelCommand	Gewährt die Berechtigung zum Abbrechen eines angegebenen Befehls „Run Command (Befehl ausführen)“.	Write			
CancelMaintenanceWindowExecution	Gewährt die Berechtigung, die laufende Ausführung eines Wartungsfensters abzubrechen.	Write	maintenancewindow*		
CreateActivation	Gewährt die Berechtigung zum Erstellen einer Aktivierung, die zum Registrieren von On-Premises-Servern und virtuellen Maschinen (VMs) bei Systems Manager verwendet wird	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssociation	Gewährt die Berechtigung, ein angegebenes Systems Manager-Dokument bestimmten Instances oder anderen Zielen zuzuordnen.	Schreiben	association*		
			document*		
			instance		
			managed-instance		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssociationBatch	Gewährt die Berechtigung zum Kombinieren von Einträgen für mehrere CreateAssociation Operationen in einem einzigen Befehl	Schreiben	document*		
			instance		
			managed-instance		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateDocument	Gewährt die Berechtigung zum Erstellen eines Systems Manager-SSM-Dokuments	Write	document*		iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMaintenanceWindow	Gewährt die Berechtigung zum Erstellen eines Wartungsfensters.	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOpsItem	Gewährt die Berechtigung zum Erstellen eines OpsItem in OpsCenter	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOpsMetadata	Gewährt die Berechtigung zum Erstellen eines OpsMetadata Objekts für eine - AWS Ressource	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePatchBaseline	Gewährt die Berechtigung zum Erstellen einer Patch-Baseline	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateResourceDataSync	Gewährt die Berechtigung zum Erstellen einer Ressourcendaten-Synchronisierungskonfiguration, die regelmäßig Bestandsdaten von verwalteten Instances sammelt und die Daten in einem Amazon-S3-Bucket aktualisiert	Write	resourcedatasync*		
				ssm:SyncType	
DeleteActivation	Gewährt die Berechtigung zum Löschen einer angegebenen Aktivierung für verwaltete Instances.	Write			
DeleteAssociation	Gewährt die Berechtigung, ein angegebenes SSM-Dokument von einer angegebenen Instance zu trennen.	Write	association		
			document		
			instance		
			managed-instance		
				aws:ResourceTag/${TagKey}	
DeleteDocument	Gewährt die Berechtigung zum Löschen eines angegebenen SSM-Dokuments und seiner Instance-Mappings.	Write	document*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteInventory	Gewährt die Berechtigung zum Löschen eines angegebenen benutzerdefinierten Bestandstyps oder der einem benutzerdefinierten Bestandstyp zugeordneten Daten.	Write			
DeleteMaintenanceWindow	Gewährt die Berechtigung zum Löschen eines angegebenen Wartungsfensters.	Schreiben	maintenancewindow*		
DeleteOpsItem	Gewährt die Berechtigung zum Löschen eines OpsItem	Schreiben	opsitem*		
DeleteOpsMetadata	Gewährt die Berechtigung zum Löschen eines OpsMetadata Objekts	Schreiben	opsmetadata*		
DeleteParameter	Gewährt die Berechtigung zum Löschen eines angegebenen SSM-Parameters.	Write	parameter*		
DeleteParameters	Gewährt die Berechtigung zum Löschen mehrerer angegebener SSM-Parameter.	Write	parameter*		
DeletePatchBaseline	Gewährt die Berechtigung zum Löschen einer angegebenen Patch-Baseline.	Write	patchbaseline*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteResourceDataSync	Gewährt die Berechtigung zum Löschen einer angegebenen Ressourcendatensynchronisierung,	Schreiben	resourcedatasync*		
				ssm:SyncType	
DeleteResourcePolicy	Gewährt die Berechtigung zum Löschen einer Systems-Manager-Ressourcenrichtlinie	Berechtigungsverwaltung	resourcearn*		
DeregisterManagedInstance	Gewährt die Berechtigung zum Abmelden von angegebenen On-Premises-Servern oder virtuellen Maschinen (VM) von Systems Manager.	Write	managed-instance*		
				ssm:resourceTag/tag-key	
DeregisterPatchBaselineForPatchGroup	Gewährt die Berechtigung, die Registrierung einer angegebenen Patch-Baseline als Standard-Patch-Baseline für eine bestimmte Patch-Gruppe aufzuheben.	Write	patchbaseline*		
DeregisterTargetFromMaintenanceWindow	Gewährt die Berechtigung, ein bestimmtes Ziel von einem Wartungsfenster abzumelden.	Write	maintenancewindow*		
DeregisterTaskFromMaintenanceWindow	Gewährt die Berechtigung, eine bestimmte Aufgabe von einem Wartungsfenster abzumelden.	Write	maintenancewindow*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeActivations	Gewährt die Berechtigung zum Anzeigen von Details zu einer angegebenen Aktivierung einer verwalteten Instance, z. B. zum Zeitpunkt der Erstellung und zur Anzahl der unter Verwendung der Aktivierung registrierten Instances.	Read			
DescribeAssociation	Gewährt die Berechtigung zum Anzeigen von Details über die angegebene Mapping für eine angegebene Instance oder ein bestimmtes Ziel.	Read	association		
			document		
			instance		
			managed-instance		
				aws:ResourceTag/${TagKey}	
DescribeAssociationExecutionTargets	Gewährt die Berechtigung zum Anzeigen von Informationen zu einer spezifischen Ausführung einer Mapping.	Read	association*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeAssociationExecutions	Gewährt die Berechtigung zum Anzeigen aller Ausführungen für eine bestimmte Mapping.	Read	association*		
				aws:ResourceTag/${TagKey}	
DescribeAutomationExecutions	Gewährt die Berechtigung zum Anzeigen von Details zu allen aktiven und beendeten Automatisierungsausführungen.	Read			
DescribeAutomationStepExecutions	Gewährt die Berechtigung zum Anzeigen von Informationen über alle aktiven und beendeten Schrittausführungen in einem Automatisierungs-Workflow.	Read	automation-execution*		
DescribeAvailablePatches	Gewährt die Berechtigung zum Anzeigen aller Patches, die in eine Patch-Baseline aufgenommen werden können.	Read			
DescribeDocument	Gewährt die Berechtigung zum Anzeigen von Details zu einem angegebenen SSM-Dokument.	Read	document*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDocumentParameters	Gewährt die Berechtigung zum Anzeigen von Informationen zu SSM-Dokumentparametern in der Systems Manager-Konsole (interne Systems Manager-Aktion).	Read	document*		
DescribeDocumentPermission	Gewährt die Berechtigung zum Anzeigen der Berechtigungen für ein bestimmtes SSM-Dokument.	Read	document*		
DescribeEffectiveInstanceAssociations	Gewährt die Berechtigung zum Anzeigen aller aktuellen Mappings für eine angegebene Instance.	Read	instance*		
			managed-instance*		
				aws:ResourceTag/${TagKey}	
DescribeEffectivePatchesForPatchBaseline	Gewährt die Berechtigung zum Anzeigen von Details zu den Patches, die derzeit mit der angegebenen Patch-Baseline verknüpft sind (nur Windows).	Read	patchbaseline*		
DescribeInstanceAssociationsStatus	Gewährt die Berechtigung zum Anzeigen des Status der Mappings für eine bestimmte Instance.	Read	instance*		
			managed-instance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
DescribeInstanceInformation	Gewährt die Berechtigung zum Anzeigen von Details zu einer angegebenen Instance.	Read			
DescribeInstancePatchStates	Gewährt die Berechtigung zum Anzeigen von Statusdetails zu Patches auf einer angegebenen Instance.	Read			
DescribeInstancePatchStatesForPatchGroup	Gewährt die Berechtigung zum Beschreiben des allgemeinen Patch-Status für die Instances in der angegebenen Patch-Gruppe	Read			
DescribeInstancePatches	Gewährt die Berechtigung zum Anzeigen allgemeiner Details zu den Patches auf einer angegebenen Instance.	Read			
DescribeInstanceProperties	Gewährt der Amazon EC2-Konsole des Benutzers die Berechtigung zum Rendern der Knoten von verwalteten Instances	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeInventoryDeletions	Gewährt die Berechtigung zum Anzeigen von Details zu einer angegebenen Lagerbestandslöschung.	Read			
DescribeMaintenanceWindowExecutionTaskInvocations	Gewährt die Berechtigung zum Anzeigen von Details einer angegebenen Aufgabenausführung für ein Wartungsfenster.	List			
DescribeMaintenanceWindowExecutionTasks	Gewährt die Berechtigung zum Anzeigen von Details zu den Aufgaben, die während der Ausführung eines bestimmten Wartungsfensters ausgeführt wurden.	List	maintenancewindow*		
DescribeMaintenanceWindowExecutions	Gewährt die Berechtigung zum Anzeigen der Ausführungen eines angegebenen Wartungsfensters.	List	maintenancewindow*		
DescribeMaintenanceWindowSchedule	Gewährt die Berechtigung zum Anzeigen von Details zu bevorstehenden Ausführungen eines angegebenen Wartungsfensters.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeMaintenanceWindowTargets	Gewährt die Berechtigung zum Anzeigen einer Liste der Ziele, die einem angegebenen Wartungsfenster zugeordnet sind.	List	maintenancewindow*		
DescribeMaintenanceWindowTasks	Gewährt die Berechtigung zum Anzeigen einer Liste der Aufgaben, die einem bestimmten Wartungsfenster zugeordnet sind.	List	maintenancewindow*		
DescribeMaintenanceWindows	Gewährt die Berechtigung zum Anzeigen von Informationen zu allen oder bestimmten Wartungsfenstern.	List			
DescribeMaintenanceWindowsForTarget	Gewährt die Berechtigung zum Anzeigen von Informationen über die Ziele des Wartungsfensters und die Aufgaben, die einer angegebenen Instance zugeordnet sind.	Auflisten			
DescribeOpsItems	Gewährt die Berechtigung zum Anzeigen von Details zu einem angegebenen OpsItems	Lesen			
DescribeParameters	Gewährt die Berechtigung zum Anzeigen von Details zu einem angegebenen SSM-Parameter.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribePatchBaselines	Gewährt die Berechtigung zum Anzeigen von Informationen zu Patch-Baselines, die die angegebenen Kriterien erfüllen.	List			
DescribePatchGroupState	Gewährt die Berechtigung zum Anzeigen aggregierter Statusdetails zu Patches für eine bestimmte Patch-Gruppe.	Auflisten			
DescribePatchGroups	Gewährt die Berechtigung zum Anzeigen von Informationen zur Patch-Baseline für eine bestimmte Patch-Gruppe.	List			
DescribePatchProperties	Gewährt die Berechtigung zum Anzeigen von Details zu verfügbaren Patches für ein bestimmtes Betriebssystem und eine Patch-Eigenschaft.	List			
DescribeSessions	Gewährt die Berechtigung zum Anzeigen einer Liste der letzten Session Manager-Sitzungen, die die angegebenen Suchkriterien erfüllen.	Auflisten			
DisassociateOpsItemRelatedItem	Gewährt die Berechtigung zum Trennen der Zuordnung RelatedItem zu einem OpsItem	Schreiben	opsitem*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAutomationExecution	Gewährt die Berechtigung zum Anzeigen von Details zu einer angegebenen Automatisierungsausführung.	Lesen	automation-execution*		
GetCalendar [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen von Details eines bestimmten Kalenders	Lesen	document*		
GetCalendarState	Gewährt die Berechtigung zum Anzeigen des Kalenderstatus für einen Änderungskalender oder eine Liste mit Änderungskalendern	Read	document*		
GetCommandInvocation	Gewährt die Berechtigung zum Anzeigen von Details zur Befehlsausführung eines angegebenen Aufrufs oder Plugins.	Read			
GetConnectionStatus	Gewährt die Berechtigung zum Anzeigen des Session Manager-Verbindungsstatus für eine angegebene verwaltete Instance.	Read	instance		
			managed-instance		
			task		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ssm:resourceTag/${TagKey} aws:ResourceTag/${TagKey}	
GetDefaultPatchBaseline	Gewährt die Berechtigung zum Anzeigen der aktuellen Standard-Patch-Baseline für einen angegebenen Betriebssystemtyp.	Read	patchbaseline*		
GetDeployablePatchSnapshotForInstance	Gewährt die Berechtigung zum Abrufen des aktuellen Patch-Baseline-Snapshots für eine angegebene Instance.	Read			
GetDocument	Gewährt die Berechtigung zum Anzeigen der Inhalte eines angegebenen SSM-Dokuments.	Read	document*		
				ssm:DocumentCategories	
GetInventory	Gewährt die Berechtigung zum Anzeigen von Instance-Bestandsdetails gemäß den angegebenen Kriterien.	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetInventorySchema	Gewährt die Berechtigung zum Anzeigen einer Liste mit Bestandsarten oder Attributnamen für einen bestimmten Bestandselementtyp.	Read			
GetMaintenanceWindow	Gewährt die Berechtigung zum Anzeigen von Details zu einem angegebenen Wartungsfenster.	Read	maintenancewindow*		
GetMaintenanceWindowExecution	Gewährt die Berechtigung zum Anzeigen von Details zur Ausführung eines bestimmten Wartungsfensters.	Read			
GetMaintenanceWindowExecutionTask	Gewährt die Berechtigung zum Anzeigen von Details zu einer bestimmten Ausführungsaufgabe im Wartungsfenster.	Read			
GetMaintenanceWindowExecutionTaskInvocation	Gewährt die Berechtigung zum Anzeigen von Details zu einer bestimmten Aufgabe im Wartungsfenster, die auf einem bestimmten Ziel ausgeführt wird.	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetMaintenanceWindowTask	Gewährt die Berechtigung zum Anzeigen von Details zu Aufgaben, die mit einem angegebenen Wartungsfenster registriert wurden.	Lesen	maintenancewindow*		
GetManifest [nur Berechtigung]	Gewährt die Berechtigung an Systems Manager und SSM Agent zum Ermitteln der Paket-Installationsanforderungen für eine Instance (interner Systems Manager-Aufruf)	Lesen			
GetOpsItem	Gewährt die Berechtigung zum Anzeigen von Informationen zu einem angegebenen OpsItem	Lesen	opsitem*		
GetOpsMetadata	Gewährt die Berechtigung zum Abrufen eines OpsMetadata Objekts	Lesen	opsmetadata*		
GetOpsSummary	Gewährt die Berechtigung zum Anzeigen von zusammenfassenden Informationen zu OpsItems basierend auf bestimmten Filtern und Aggregatoren	Lesen	resourcedatasync*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetParameter	Gewährt die Berechtigung zum Anzeigen von Informationen zu einem angegebenen Parameter.	Read	parameter*		
GetParameterHistory	Gewährt die Berechtigung zum Anzeigen von Details und Änderungen für einen angegebenen Parameter.	Read	parameter*		
GetParameters	Gewährt die Berechtigung zum Anzeigen von Informationen über mehrere angegebene Parameter.	Read	parameter*		
GetParametersByPath	Gewährt die Berechtigung zum Anzeigen von Informationen über Parameter in einer angegebenen Hierarchie.	Read	parameter*		
				ssm:Recursive	
GetPatchBaseline	Gewährt die Berechtigung zum Anzeigen von Informationen über eine angegebene Patch-Baseline.	Read	patchbaseline*		
GetPatchBaselineForPatchGroup	Gewährt die Berechtigung zum Anzeigen der ID der aktuellen Patch-Baseline für eine angegebene Patch-Gruppe.	Lesen	patchbaseline*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetResourcePolicies	Gewährt die Berechtigung zum Abrufen von Listen mit Systems-Manager-Ressourcenrichtlinien	Auflisten	resourcearn*		
GetServiceSetting	Gewährt die Berechtigung zum Anzeigen der Einstellung auf Kontoebene für einen - AWS Service	Lesen	servicesetting*		
LabelParameterVersion	Gewährt die Berechtigung zum Anwenden einer identifizierenden Bezeichnung auf eine angegebene Version eines Parameters.	Write	parameter*		
ListAssociationVersions	Gewährt die Berechtigung zum Auflisten von Versionen der angegebenen Mapping	List	association*		
				aws:ResourceTag/${TagKey}	
ListAssociations	Gewährt die Berechtigung zum Auflisten der Mappings für ein angegebenes SSM-Dokument oder eine verwaltete Instance.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListCommandInvocations	Gewährt die Berechtigung zum Auflisten von Informationen zu Befehlsaufrufen, die an eine angegebene Instance gesendet wurden.	Auflisten			
ListCommands	Gewährt die Berechtigung zum Auflisten der an eine angegebene Instance gesendeten Befehle.	Auflisten			
ListComplianceItems	Gewährt die Berechtigung zum Auflisten des Compliance-Status für bestimmte Ressourcentypen auf einer angegebenen Ressource.	List			
ListComplianceSummaries	Gewährt die Berechtigung zum Auflisten einer zusammenfassenden Anzahl von konformen und nicht konformen Ressourcen für einen angegebenen Compliance-Typ.	List			
ListDocumentMetadataHistory	Gewährt die Berechtigung zum Anzeigen des Metadatenverlaufs zu einem bestimmten SSM-Dokument	Auflisten	document*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDocumentVersions	Gewährt die Berechtigung zum Auflisten aller Versionen eines angegebenen Dokuments.	List	document*		
ListDocuments	Gewährt die Berechtigung zum Anzeigen von Informationen zu einem angegebenen SSM-Dokument.	Auflisten			
ListInstanceAssociations	Gewährt dem SSM Agent die Berechtigung, nach neuen Statusmanager-Zuordnungen zu suchen (interner Systems-Manager-Aufruf)	Auflisten	instance		
			managed-instance		
				aws:ResourceTag/${TagKey}	
ListInventoryEntries	Gewährt die Berechtigung zum Anzeigen einer Liste der angegebenen Bestandstypen für eine angegebene Instance.	Auflisten			
ListOpsItemEvents	Gewährt die Berechtigung zum Anzeigen von Details zu OpsItemEvents	Auflisten			
ListOpsItemRelatedItems	Gewährt die Berechtigung zum Anzeigen von Details zu OpsItem RelatedItems	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListOpsMetadata	Gewährt die Berechtigung zum Anzeigen einer Liste von OpsMetadata Objekten	Auflisten			
ListResourceComplianceSummaries	Gewährt die Berechtigung zum Auflisten von Summenzählungen auf Ressourcenebene	List			
ListResourceDataSync	Gewährt die Berechtigung zum Auflisten von Informationen zu Ressourcendaten-Synchronisierungskonfigurationen in einem Konto.	List		ssm:SyncType	
ListTagsForResource	Gewährt die Berechtigung zum Anzeigen einer Liste von Ressourcen-Tags für eine angegebene Ressource.	Auflisten	association		
			automation-execution		
			document		
			maintenancewindow		
			managed-instance		
			opsitem		
			opsmetadata		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			parameter		
			patchbaseline		
				aws:ResourceTag/${TagKey}	
ModifyDocumentPermission	Gewährt die Berechtigung, ein benutzerdefiniertes SSM-Dokument öffentlich oder privat für bestimmte AWS Konten freizugeben	Berechtigungsverwaltung	document*		
PutCalendar [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen/Bearbeiten eines bestimmten Kalenders	Schreiben	document*		
PutComplianceItems	Gewährt die Berechtigung zum Registrieren eines Compliance-Typs und anderer Compliance-Details zu einer bestimmten Ressource.	Schreiben	instance		
			managed-instance		
				ssm:SourceInstanceARN	
				ec2:SourceInstanceARN	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutConfigurePackageResult [nur Berechtigung]	Gewährt dem SSM Agent die Berechtigung, einen Bericht über die Ergebnisse bestimmter Agentenanforderungen zu generieren (interner Systems-Manager-Aufruf)	Lesen			
PutInventory	Gewährt die Berechtigung zum Hinzufügen oder Aktualisieren von Bestandselementen auf mehreren angegebenen verwalteten Instances.	Write			
PutParameter	Gewährt die Berechtigung zum Erstellen eines SSM-Parameters	Schreiben	parameter*		
				aws:RequestTag/${TagKey} aws:TagKeys ssm:Overwrite	
PutResourcePolicy	Gewährt die Berechtigung zum Erstellen oder Aktualisieren einer Systems-Manager-Ressourcenrichtlinie	Berechtigungsverwaltung	resourcearn*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RegisterDefaultPatchBaseline	Gewährt die Berechtigung zur Angabe der Standard-Patch-Baseline für einen Betriebssystemtyp.	Schreiben	patchbaseline*		
RegisterManagedInstance	Gewährt die Berechtigung zum Registrieren eines Systems Manager Agent	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
RegisterPatchBaselineForPatchGroup	Gewährt die Berechtigung zur Angabe der Standard-Patch-Baseline für eine bestimmte Patch-Gruppe.	Write	patchbaseline*		
RegisterTargetWithMaintenanceWindow	Gewährt die Berechtigung zum Registrieren eines Ziels in einem angegebenen Wartungsfenster.	Write	maintenancewindow*		
RegisterTaskWithMaintenanceWindow	Gewährt die Berechtigung zum Registrieren einer Aufgabe in einem angegebenen Wartungsfenster.	Write	maintenancewindow*		
RemoveTagsFromResource	Gewährt die Berechtigung zum Entfernen eines angegebenen Tag-Schlüssels aus einer angegebenen Ressource.	Tagging	association		
			automation-execution		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			document		
			instance		
			maintenancewindow		
			managed-instance		
			opsitem		
			opsmetadata		
			parameter		
			patchbaseline		
			task		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ResetServiceSetting	Gewährt die Berechtigung zum Zurücksetzen der Serviceeinstellung für einen AWS-Konto auf den Standardwert	Schreiben	servicesetting*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ResumeSession	Gewährt die Berechtigung zum Wiederherstellen einer Session Manager-Sitzung mit einer verwalteten Instance.	Write	session*		
				ssm:resourceTag/aws:ssmmessages:session-id ssm:resourceTag/aws:ssmmessages:target-id	
SendAutomationSignal	Gewährt die Berechtigung zum Senden eines Signals, um das aktuelle Verhalten oder den Status einer angegebenen Automatisierungsausführung zu ändern.	Write	automation-execution*		
SendCommand	Gewährt die Berechtigung zum Ausführen von Befehlen auf einer oder mehreren angegebenen verwalteten Instances.	Write	document*		
			bucket		
			instance		
			managed-instance		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}	
StartAssociationsOnce	Gewährt die Berechtigung zum manuellen Ausführen einer bestimmten Mapping.	Write	association*		
				aws:ResourceTag/${TagKey}	
StartAutomationExecution	Gewährt die Berechtigung zum Initiieren der Ausführung eines Automation-Dokuments.	Write	automation-definition*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartChangeRequestExecution	Gewährt die Berechtigung zum Initiieren der Ausführung eines Automation Change Template-Dokuments	Write	automation-definition*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys ssm:AutoApprove	
StartSession	Gewährt die Berechtigung zum Initiieren einer Verbindung zu einem angegebenen Ziel für eine Session Manager-Sitzung.	Write	document		
			instance		
			managed-instance		
			task		
				ssm:SessionDocumentAccessCheck ssm:resourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StopAutomationExecution	Gewährt die Berechtigung zum Beenden einer angegebenen Automatisierungsausführung, die bereits läuft.	Write	automation-execution*		
TerminateSession	Gewährt die Berechtigung zum dauerhaften Beenden einer Session Manager-Verbindung zu einer Instance	Schreiben	session*		
				ssm:resourceTag/aws:ssmmessages:session-id ssm:resourceTag/aws:ssmmessages:target-id	
UnlabelParameterVersion	Gewährt die Berechtigung zum Anwenden einer identifizierenden Bezeichnung auf eine angegebene Version eines Parameters	Schreiben	parameter*		
UpdateAssociation	Gewährt die Berechtigung zum Aktualisieren einer Mapping und zum sofortigen Ausführen der Mapping auf den angegebenen Zielen.	Write	association*		
			document		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			instance		
			managed-instance		
				aws:ResourceTag/${TagKey}	
UpdateAssociationStatus	Gewährt die Berechtigung zum Aktualisieren des Status des SSM-Dokuments, das einer bestimmten Instance zugeordnet ist.	Write	document*		
			instance		
			managed-instance		
				ssm:SourceInstanceARN ec2:SourceInstanceARN aws:ResourceTag/${TagKey}	
UpdateDocument	Gewährt die Berechtigung zum Aktualisieren eines oder mehrerer Werte für ein SSM-Dokument.	Write	document*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateDocumentDefaultVersion	Gewährt die Berechtigung zum Ändern der Standardversion eines SSM-Dokuments.	Write	document*		
UpdateDocumentMetadata	Gewährt die Berechtigung zum Aktualisieren der Metadaten eines SSM-Dokuments	Schreiben	document*		
UpdateInstanceAssociationStatus [nur Berechtigung]	Gewährt dem SSM Agent die Berechtigung, den Status der aktuell ausgeführten Zuordnung zu aktualisieren (interner Systems-Manager-Aufruf)	Schreiben	association*		
			instance		
			managed-instance		
				ssm:SourceInstanceARN ec2:SourceInstanceARN aws:ResourceTag/${TagKey}	
UpdateInstanceInformation	Gewährt dem SSM Agent die Berechtigung, ein Heartbeat-Signal an den Systems-Manager-Service in der Cloud zu senden	Schreiben	instance		
			managed-instance		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				ssm:SourceInstanceARN ec2:SourceInstanceARN	
UpdateMaintenanceWindow	Gewährt die Berechtigung zum Aktualisieren eines angegebenen Wartungsfensters.	Write	maintenancewindow*		
UpdateMaintenanceWindowTarget	Gewährt die Berechtigung zum Aktualisieren eines angegebenen Wartungsfensterziels.	Write	maintenancewindow*		
			windowtarget*		
UpdateMaintenanceWindowTask	Gewährt die Berechtigung zum Aktualisieren einer angegebenen Wartungsfensteraufgabe.	Write	maintenancewindow*		
			windowtask*		
UpdateManagedInstanceRole	Gewährt die Berechtigung zum Zuweisen oder Ändern der IAM-Rolle, die einer angegebenen verwalteten Instance zugewiesen ist.	Schreiben	managed-instance*		
				ssm:resourceTag/tag-key	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateOpsItem	Gewährt die Berechtigung zum Bearbeiten oder Ändern eines OpsItem	Schreiben	opsitem*		
UpdateOpsMetadata	Gewährt die Berechtigung zum Aktualisieren eines OpsMetadata Objekts	Schreiben	opsmetadata*		
UpdatePatchBaseline	Gewährt die Berechtigung zum Aktualisieren einer angegebenen Patch-Baseline.	Write	patchbaseline*		
UpdateResourceDataSync	Gewährt die Berechtigung zum Aktualisieren einer Ressourcendaten-Synchronisierung	Schreiben	resourcedatasync*		
				ssm:SyncType	
UpdateServiceSetting	Gewährt die Berechtigung zum Aktualisieren der Service-Einstellung für ein AWS-Konto	Schreiben	servicesetting*		

Von AWS Systems Manager definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

> **Note**
>
> Einige State Manager-API-Parameter sind veraltet. Das könnte ein unerwartetes Verhalten verursachen. Weitere Informationen finden Sie unter Arbeiten mit Mappings mithilfe von IAM.

Ressource ntypen	ARN	Bedingungsschlüssel
association	`arn:${Partition}:ssm:${Region}:${Account}:association/${AssociationId}`	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
automation-execution	`arn:${Partition}:ssm:${Region}:${Account}:automation-execution/${AutomationExecutionId}`	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
automation-definition	`arn:${Partition}:ssm:${Region}:${Account}:automation-definition/${AutomationDefinitionName}:${VersionId}`	
bucket	`arn:${Partition}:s3:::${BucketName}`	
document	`arn:${Partition}:ssm:${Region}:${Account}:document/${DocumentName}`	aws:ResourceTag/${TagKey} ssm:DocumentCategories ssm:resourceTag/${TagKey}
instance	`arn:${Partition}:ec2:${Region}:${Account}:instance/${InstanceId}`	aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
maintenancewindow	arn:${Partition}:ssm:${Region}:${Account}:maintenancewindow/${ResourceId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
managed-instance	arn:${Partition}:ssm:${Region}:${Account}:managed-instance/${InstanceId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
managed-instance-inventory	arn:${Partition}:ssm:${Region}:${Account}:managed-instance-inventory/${InstanceId}	
opsitem	arn:${Partition}:ssm:${Region}:${Account}:opsitem/${ResourceId}	aws:ResourceTag/${TagKey}
opsmetadata	arn:${Partition}:ssm:${Region}:${Account}:opsmetadata/${ResourceId}	aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}
parameter	arn:${Partition}:ssm:${Region}:${Account}:parameter/${ParameterNameWithoutLeadingSlash}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
patchbaseline	arn:${Partition}:ssm:${Region}:${Account}:patchbaseline/${PatchBaselineIdResourceId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key

Ressourcentypen	ARN	Bedingungsschlüssel
resourcearn	arn:${Partition}:ssm:${Region}:${Account}:opsitemgroup/default	
session	arn:${Partition}:ssm:${Region}:${Account}:session/${SessionId}	ssm:resourceTag/aws:ssmmessages:session-id ssm:resourceTag/aws:ssmmessages:target-id
resourcedatasync	arn:${Partition}:ssm:${Region}:${Account}:resource-data-sync/${SyncName}	
servicesetting	arn:${Partition}:ssm:${Region}:${Account}:servicesetting/${ResourceId}	
windowtarget	arn:${Partition}:ssm:${Region}:${Account}:windowtarget/${WindowTargetId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
windowtask	arn:${Partition}:ssm:${Region}:${Account}:windowtask/${WindowTaskId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
task	arn:${Partition}:ecs:${Region}:${Account}:task/${TaskId}	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Systems Manager

AWS Systems Manager definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die

Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Create-Anforderungen basierend auf den zulässigen Werten für die angegebenen Tags	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf einem Tag-Schlüssel-Wert-Paar, das der AWS Ressource zugewiesen ist	String
aws:TagKeys	Filtert den Zugriff nach Create-Anforderungen basierend darauf, ob obligatorische Tags in der Anforderung enthalten sind	ArrayOfString
ec2:SourceInstanceARN	Filtert den Zugriff nach ARN der Instance, von der die Anforderung stammt	ARN
ssm:AutoApprove	Filtert den Zugriff, indem überprüft wird, ob ein Benutzer berechtigt ist, Change Manager-Workflows ohne Überprüfungsschritt zu starten (mit Ausnahme von Ereignissen zum Einfrieren von Änderungen)	Bool
ssm:DocumentCategories	Filtert den Zugriff, indem überprüft wird, ob ein Benutzer berechtigt ist, auf ein Dokument zuzugreifen, das zu einer bestimmten Kategorieaufzählung gehört.	ArrayOfString
ssm:Overwrite	Filtert den Zugriff durch Steuerung, ob Systems-Manager-Parameter überschrieben werden können	String
ssm:Recursive	Filtert den Zugriff nach Systems-Manager-Parametern, die in einer hierarchischen Struktur erstellt wurden	String

Bedingungsschlüssel	Beschreibung	Typ
ssm:SessionDocumentAccessCheck	Filtert den Zugriff, indem überprüft wird, ob ein Benutzer berechtigt ist, entweder auf das Standardkonfigurationsdokument von Session Manager oder auf das in einer Anforderung angegebene benutzerdefinierte Konfigurationsdokument zuzugreifen	Bool
ssm:SourceInstanceARN	Filtert den Zugriff, indem der Amazon-Ressourcenname (ARN) der verwalteten Instance des AWS Systems Managers überprüft wird, von der aus die Anforderung gestellt wird. Dieser Schlüssel ist nicht vorhanden, wenn die Instance von der verwalteten Instance kommt, die mit einer IAM-Rolle authentifiziert wurde, die dem EC2-Instance-Profil zugeordnet ist	ARN
ssm:SyncType	Filtert den Zugriff, indem überprüft wird, ob ein Benutzer auch Zugriff auf die in der Anforderung ResourceDataSync SyncType angegebenen hat	String
ssm:resourceTag/${TagKey}	Filtert den Zugriff nach einem Tag-Schlüssel-Wert-Paar, das der Systems-Manager-Ressource zugewiesen ist	String
ssm:resourceTag/aws:ssmmessages:session-id	Filtert den Zugriff basierend auf einem Tag-Schlüssel-Wert-Paar, das der Systems-Manager-Sitzungsressource zugewiesen ist	String
ssm:resourceTag/aws:ssmmessages:target-id	Filtert den Zugriff basierend auf einem Tag-Schlüssel-Wert-Paar, das der Systems-Manager-Sitzungsressource zugewiesen ist	String
ssm:resourceTag/tag-key	Filtert den Zugriff basierend auf einem Tag-Schlüssel-Wert-Paar, das der Systems-Manager-Ressource zugewiesen ist	String

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Systems Manager für SAP

AWS Systems Manager for SAP (Dienstpräfix:`ssm-sap`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Systems Manager für SAP definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie

den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BackupDatabase	Gewährt die Berechtigung zum Ausführen eines Backup-Vorgangs für eine bestimmte Datenbank	Schreiben			
DeleteResourcePermission	Gewährt die Berechtigung zum Löschen der mit einer SSM für SAP-Datenbankressource verknüpften Ressourcenberechtigungen auf SSM-Ebene für SAP-Ebene	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeregisterApplication	Gewährt die Berechtigung zum Aufheben der Registrierung einer SAP-Anwendung für SAP	Schreiben	application		
GetApplication	Gewährt die Berechtigung zum Zugreifen auf Informationen über eine bei SSM für SAP registrierte Anwendung, indem die Anwendungs-ID oder der Anwendungs-ARN angegeben werden	Lesen			
GetComponent	Gewährt die Berechtigung zum Zugreifen auf Informationen über eine bei SSM für SAP registrierte Komponente, indem die Anwendungs-ID und die Komponenten-ID angegeben werden	Lesen	component		
GetDatabase	Gewährt die Berechtigung zum Zugreifen auf Informationen über eine bei SSM für SAP registrierte Datenbank, indem die Anwendungs-ID, Komponenten-ID und Datenbank-ID angegeben werden	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetOperation	Gewährt die Berechtigung zum Zugreifen auf Informationen zu einer Operation, indem die angegebene Vorgangs-ID	Lesen			
GetResourcePermission	Gewährt die Berechtigung zum Abrufen der mit einer SSM für SAP-Datenbankressource verknüpften Ressourcenberechtigungen auf SSM-Ebene für SAP-Ebene	Lesen			
ListApplications	Erteilt die Berechtigung, eine Liste aller beim Kunden bei SSM for SAP registrierten Anwendungen abzurufen AWS-Konto	Auflisten			
ListComponents	Gewährt die Berechtigung zum Abrufen einer Liste aller Komponenten des Kundenkontos oder einer bestimmten Anwendung	Auflisten	application		
ListDatabases	Gewährt die Berechtigung zum Abrufen einer Liste aller Datenbanken im Konto des Kunden oder einer bestimmten Anwendung	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListOperationEvents	Erteilt die Berechtigung zum Abrufen einer Liste aller Vorgangsereignisse in einem angegebenen Vorgang	Auflisten			
ListOperations	Gewährt die Berechtigung zum Abrufen einer Liste aller Kundenkonten, zusätzliche Filter können angewendet werden	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für den angegebenen Ressourcen-ARN	Lesen			
PutResourcePermission	Gewährt die Berechtigung zum Hinzufügen von Ressourcenberechtigungen auf SSM-Ebene für SAP-Ebene, die einer SSM für SAP-Datenbankressource zugeordnet sind	Schreiben			
RegisterApplication	Gewährt die Berechtigung zum Registrieren einer SAP-Anwendung bei SSM für SAP	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RestoreDatabase	Gewährt die Berechtigung zum Wiederherstellen einer Datenbank aus einer anderen Datenbank	Schreiben			
StartApplication	Erteilt die Erlaubnis, eine registrierte SSM-Anwendung für SAP zu starten	Schreiben	application		
StartApplicationRefresh	Gewährt die Berechtigung zum Starten einer On-Demand-Erkennung einer registrierten SSM für SAP-Anwendung	Schreiben	application		
StopApplication	Erteilt die Berechtigung, eine registrierte SSM für SAP-Anwendung zu beenden	Schreiben	application		
TagResource	Gewährt die Berechtigung zum Markieren eines angegebenen Ressourcen-ARNs	Tagging	application		
			component		
			database		
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus dem angegebenen Ressourcen-ARN	Tagging	application		
			component		
			database		
				aws:TagKeys	
UpdateApplicationSettings	Gewährt die Berechtigung zum Aktualisieren der registrierten SSM für SAP-Anwendung	Schreiben	application		
UpdateHANABackupSettings	Gewährt die Berechtigung zum Aktualisieren der HANA-Sicherungseinstellungen einer angegebenen Datenbank	Schreiben			

Von AWS Systems Manager für SAP definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
application	`arn:${Partition}:ssm-sap:${Region}:${Account}:${ApplicationType}/${ApplicationId}`	aws:ResourceTag/${TagKey}
component	`arn:${Partition}:ssm-sap:${Region}:${Account}:${ApplicationType}/${ApplicationId}/COMPONENT/${ComponentId}`	aws:ResourceTag/${TagKey}
database	`arn:${Partition}:ssm-sap:${Region}:${Account}:${ApplicationType}/${ApplicationId}/DB/${DatabaseId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Systems Manager für SAP

AWS Systems Manager for SAP definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Systems Manager GUI Connect

AWS Systems Manager GUI Connect (Servicepräfix: `ssm-guiconnect`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Systems Manager GUI Connect definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie

den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelConnection [nur Berechtigung]	Gewährt die Berechtigung zum Beenden einer GUI Connect-Verbindung	Schreiben			
GetConnection [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen der Metadaten für eine GUI Connect-Verbindung	Lesen			
StartConnection [nur Berechtigung]	Gewährt die Berechtigung zum Starten einer GUI Connect-Verbindung	Schreiben			

Von AWS Systems Manager GUI Connect definierte Ressourcentypen

AWS Systems Manager GUI Connect unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf AWS Systems Manager GUI Connect zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Systems Manager GUI Connect

GUI Connect hat keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager (Servicepräfix: `ssm-incidents`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Systems Manager Incident Manager definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den

Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetIncidentFindings	Gewährt die Berechtigung zum Abrufen von Details zu bestimmten Ergebnissen für einen Vorfalldatensatz	Lesen	incident-record*		
			response-plan*		
CreateReplicationSet	Gewährt die Berechtigung zum Erstellen eines Replikationssatzes	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole ssm-incidents:TagResource
CreateResponsePlan	Gewährt die Berechtigung zum Erstellen eines Reaktionsplans	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:PassRole ssm-incidents:TagResource
CreateTimelineEvent	Gewährt die Berechtigung zum Erstellen eines Zeitleistenereignisses für einen Vorfalldatensatz	Write	incident-record*		
			response-plan*		
DeleteIncidentRecord	Gewährt die Berechtigung zum Löschen eines Vorfalldatensatzes	Write	incident-record*		
DeleteReplicationSet	Gewährt die Berechtigung zum Löschen eines Replikationssatzes	Write	replication-set*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteResourcePolicy	Gewährt die Berechtigung zum Löschen von Ressourcenrichtlinien aus einem Reaktionsplans	Berechtigungsverwaltung	response-plan*		
DeleteResponsePlan	Gewährt die Berechtigung zum Löschen eines Reaktionsplans	Write	response-plan*		
DeleteTimelineEvent	Gewährt die Berechtigung zum Löschen eines Zeitleistenereignisses	Write	incident-record*		
GetIncidentRecord	Gewährt die Berechtigung zum Anzeigen des Inhalts eines Vordatensatzes	Read	incident-record*		
			response-plan*		
GetReplicationSet	Gewährt die Berechtigung zum Beenden des Replikationssatzes	Read	replication-set*		
GetResourcePolicies	Gewährt die Berechtigung zum Anzeigen von Ressourcenrichtlinien eines Reaktionsplans	Read	response-plan*		
GetResponsePlan	Gewährt die Berechtigung zum Anzeigen der Inhalte eines angegebenen Reaktionsplans	Read	response-plan*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetTimelineEvent	Gewährt die Berechtigung zum Anzeigen eines Zeitleistenereignisses	Lesen	incident-record*		
			response-plan*		
ListIncidentFindings	Gewährt die Berechtigung zum Auflisten von Ergebnissen für einen Vorfalldatensatz	Auflisten	incident-record*		
			response-plan*		
ListIncidentRecords	Gewährt die Berechtigung zum Auflisten des Inhalts aller Vorfalldatensätze	Auflisten			
ListRelatedItems	Gewährt die Berechtigung zum Auflisten zugehöriger Elemente eines Vorfallsdatensatzes	Auflisten	incident-record*		
			response-plan*		
ListReplicationSets	Gewährt die Berechtigung zum Auflisten aller Replikationssätze	List			
ListResponsePlans	Gewährt die Berechtigung zum Auflisten aller Reaktionspläne	List			
ListTagsForResource	Gewährt die Berechtigung zum Anzeigen einer Liste von Ressourcen-Tags für eine angegebene Ressource.	Read	incident-record		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			replication-set		
			response-plan		
ListTimelineEvents	Gewährt die Berechtigung zum Auflisten aller Zeitplaneignisse für einen Vorfalldatensatz	List	incident-record*		
			response-plan*		
PutResourcePolicy	Gewährt die Berechtigung zum Setzen der Ressourcenrichtlinie auf einen Reaktionsplan	Berechtigungsverwaltung	response-plan*		
StartIncident	Gewährt die Erlaubnis, einen neuen Vorfall mit einem Antwortplan zu beginnen	Write	response-plan*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einem Reaktionsplan	Markieren	incident-record		
			replication-set		
			response-plan		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einem Reaktionsplan	Markieren	incident-record		
			replication-set		
			response-plan		
				aws:TagKeys	
UpdateDeletionProtection	Gewährt die Berechtigung zum Aktualisieren des Löschschutzes für den Replikationssatz	Write	replication-set*		
UpdateIncidentRecord	Gewährt die Berechtigung zum Aktualisieren der Inhalte eines Vorfalldatensatzes	Write	incident-record*		
			response-plan*		
UpdateRelatedItems	Gewährt die Berechtigung zum Aktualisierung zugehöriger Elemente eines Vorfalldatensatzes	Write	incident-record*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			response-plan*		
UpdateReplicationSet	Gewährt die Berechtigung zum Aktualisieren eines Replikationssatzes	Write	replication-set*		
UpdateResponsePlan	Gewährt die Berechtigung zum Aktualisieren der Inhalte eines Reaktionsplans	Write	response-plan*		iam:PassRole ssm-incidents:TagResource
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateTimelineEvent	Gewährt die Berechtigung zum Aktualisieren eines Zeitplanereignisses	Write	incident-record*		
			response-plan*		

Von AWS Systems Manager Incident Manager definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
response-plan	`arn:${Partition}:ssm-incidents::${Account}:response-plan/${ResponsePlan}`	aws:ResourceTag/${TagKey}
incident-record	`arn:${Partition}:ssm-incidents::${Account}:incident-record/${ResponsePlan}/${IncidentRecord}`	aws:ResourceTag/${TagKey}
replication-set	`arn:${Partition}:ssm-incidents::${Account}:replication-set/${ReplicationSet}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Systems Manager Incident Manager Contacts

AWS Systems Manager Incident Manager Contacts (Service-Prefix: `ssm-contacts`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Systems Manager Incident Manager Contacts definierte Aktionen
- Von AWS Systems Manager Incident Manager Contacts definierte Ressourcentypen
- Bedingungsschlüssel für AWS Systems Manager Incident Manager Contacts

Von AWS Systems Manager Incident Manager Contacts definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptPage	Gewährt die Berechtigung zum Annehmen einer Seite	Write	page*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ActivateContactChannel	Gewährt die Berechtigung zum Aktivieren des Kontaktkanals eines Kontakts	Write	contactchannel*		
AssociateContact [nur Berechtigung]	Gewährt die Berechtigung zur Verwendung eines Kontakts in einem Eskalationsplan	Berechtigungsverwaltung	contact*		
CreateContact	Gewährt die Berechtigung zum Erstellen eines Kontakts	Write	contact*		ssm-contacts:AssociateContact
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateContactChannel	Gewährt die Berechtigung zum Erstellen eines Kontaktkanals für einen Kontakt	Schreiben	contact*		
CreateRotation	Gewährt die Berechtigung zum Erstellen einer Rotation in einem Bereitschaftsplan	Schreiben	rotation*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateRotationOverride	Gewährt die Berechtigung zum Überschreiben einer Rotation in einem Bereitschaftsplan	Schreiben	rotation*		
DeactivateContactChannel	Gewährt die Berechtigung zum Deaktivieren des Kontaktkanals eines Kontakts	Write	contactchannel*		
DeleteContact	Gewährt die Berechtigung zum Löschen eines Kontakts	Write	contact*		
DeleteContactChannel	Gewährt die Berechtigung zum Löschen des Kontaktkanals eines Kontakts	Schreiben	contactchannel*		
DeleteRotation	Gewährt die Berechtigung zum Löschen einer Rotation	Schreiben	rotation*		
DeleteRotationOverride	Gewährt die Berechtigung zum Löschen der Überschreibung einer Rotation	Schreiben	rotation*		
DescribeEngagement	Gewährt die Berechtigung zum Beschreiben eines Engagements	Read	engagement*		
DescribePage	Gewährt die Berechtigung zum Beschreiben einer Seite	Read	page*		
GetContact	Gewährt die Berechtigung zum Abrufen eines Kontakts	Read	contact*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetContactChannel	Gewährt die Berechtigung zum Abrufen des Kontaktkanals eines Kontakts	Lesen	contactchannel*		
GetContactPolicy	Gewährt die Berechtigung zum Abrufen der Ressourcenrichtlinie eines Kontakts	Lesen	contact*		
GetRotation	Gewährt die Berechtigung zum Abrufen von Informationen über eine Bereitschaftsrotation	Lesen	rotation*		
GetRotationOverride	Gewährt die Berechtigung zum Abrufen von Informationen über eine Überschreitung in einer Bereitschaftsrotation	Lesen	rotation*		
ListContactChannels	Gewährt die Berechtigung zum Auflisten aller Kontaktkanäle eines Kontakts	List	contact*		
ListContacts	Gewährt die Berechtigung zum Auflisten aller Kontakte	List			
ListEngagements	Gewährt die Berechtigung zum Auflisten aller Engagements	List			
ListPageReceipts	Gewährt die Berechtigung zum Auflisten aller Quittungen einer Seite	Auflisten	page*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListPageResolutions	Gewährt die Berechtigung, den Lösungspfad einer Bindung aufzulisten	Auflisten	page*		
ListPagesByContact	Gewährt die Berechtigung aller an einen Kontakt gesendeten Seiten	List	contact*		
ListPagesByEngagement	Gewährt die Berechtigung zum Auflisten aller in einem Engagement erstellten Seiten	Auflisten	engagement*		
ListPreviewRotationShifts	Gewährt die Berechtigung zum Abrufen einer Schichtliste basierend auf den Konfigurationsparametern für die Rotation	Auflisten	rotation*		
ListRotationOverrides	Gewährt die Berechtigung zum Abrufen einer Liste von Überschreibungen, die derzeit für eine Bereitschaftsrotation festgelegt sind	Auflisten	rotation*		
ListRotationShifts	Gewährt die Berechtigung zum Abrufen einer Liste von Rotationsschichten in einem Bereitschaftsplan	Auflisten	rotation*		
ListRotations	Gewährt die Berechtigung zum Abrufen einer Liste von Bereitschaftsrotationen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Anzeigen einer Liste von Ressourcen-Tags für eine angegebene Ressource.	Lesen	contact		
			rotation		
PutContactPolicy	Gewährt die Berechtigung zum Hinzufügen einer Ressourcenrichtlinie an einen Kontakt	Write	contact*		
SendActivationCode	Gewährt die Berechtigung zum Senden des Aktivierungscodes des Kontaktkanals eines Kontakts	Write	contactchannel*		
StartEngagement	Gewährt die Berechtigung zum Starten eines Engagements	Write	contact*		
StopEngagement	Gewährt die Berechtigung zum Stoppen eines Engagements	Schreiben	engagement*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zur angegebenen Ressource	Markierung	contact		
			rotation		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus der angegebenen Ressource	Markierung	contact		
			rotation		
				aws:TagKeys	
UpdateContact	Gewährt die Berechtigung zum Aktualisieren eines Kontakts	Write	contact*		ssm-contacts:AssociateContact
UpdateContactChannel	Gewährt die Berechtigung zum Aktualisieren des Kontaktkanals eines Kontakts	Schreiben	contactchannel*		
UpdateRotation	Gewährt die Berechtigung zum Aktualisieren der für eine Bereitschaftsrotation angegebenen Informationen	Schreiben	rotation*		

Von AWS Systems Manager Incident Manager Contacts definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
contact	arn:${Partition}:ssm-contacts:${Region}:${Account}:contact/${ContactAlias}	aws:ResourceTag/${TagKey}
contactchannel	arn:${Partition}:ssm-contacts:${Region}:${Account}:contactchannel/${ContactAlias}/${ContactChannelId}	
engagement	arn:${Partition}:ssm-contacts:${Region}:${Account}:engagement/${ContactAlias}/${EngagementId}	
page	arn:${Partition}:ssm-contacts:${Region}:${Account}:page/${ContactAlias}/${PageId}	
rotation	arn:${Partition}:ssm-contacts:${Region}:${Account}:rotation/${RotationId}	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Systems Manager Incident Manager Contacts

AWS Systems Manager Incident Manager Contacts definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Tag-Editor

Tag Editor (Servicepräfix: `resource-explorer`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Vom Tag-Editor definierte Aktionen
- Vom Tag-Editor definierte Ressourcentypen
- Bedingungsschlüssel für Tag-Editor

Vom Tag-Editor definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen.

Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListResourceTypes [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen der Ressourcentypen, die derzeit vom Tag-Editor unterstützt werden.	List			
ListResources [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen der Identifikatoren der Ressourcen in dem AWS-Konto	List			
ListTags [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen der Tags, die an die angegebenen Ressourcenbezeichner angefügt sind.	Read			tag:GetResources

Vom Tag-Editor definierte Ressourcentypen

Der Tag-Editor unterstützt nicht die Angabe eines Ressourcen-ARN im -`Resource`Element einer IAM-Richtlinienanweisung. Um den Zugriff auf den Tag-Editor zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für Tag-Editor

Tag-Editor besitzt keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Tax Settings

AWS Tax Settings (Servicepräfix: `tax`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Tax Settings definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchPutTaxRegistration [nur Berechtigung]	Gewährt die Berechtigung zum gebündelten Aktualisieren von Steuerregistrierungen	Schreiben			
DeleteTaxRegistration [nur Berechtigung]	Gewährt die Berechtigung zum Löschen von Steuerregistrierungsdaten	Schreiben			
GetExemptions [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen von Steuerbefreiungsdaten	Lesen			
GetTaxInfoReportingDocument [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen/Herunterladen von Steuerdokumenten/Formularen	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetTaxInheritance [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen des Steuererbstatus	Lesen			
GetTaxInterview [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Daten eines Datasatzes	Lesen			
GetTaxRegistration [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen von Steuerdaten	Lesen			
GetTaxRegistrationDocument [nur Berechtigung]	Gewährt die Berechtigung zum Herunterladen von Steuerregistrierungsdokumenten	Lesen			
ListTaxRegistrations [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen von Steuerregistrierungen	Lesen			
PutTaxInheritance [nur Berechtigung]	Gewährt die Berechtigung zum Einrichten des Steuererbes	Schreiben			
PutTaxInterview [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren von Steuerinterviewdaten	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutTaxRegistration [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren von Steuerdaten	Schreiben			
UpdateExemptions [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren von Steuerbefreiungsdaten	Schreiben			

Von AWS Tax Settings definierte Ressourcentypen

AWS Tax Settings unterstützen die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung nicht. Um den Zugriff auf AWS Tax Settings zuzulassen, geben Sie `"Resource": "*"` in der Richtlinie an.

Bedingungsschlüssel für AWS Tax Settings

Tax Settings umfasst keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Telco Network Builder

AWS Telco Network Builder (Servicepräfix: `tnb`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Telco Network Builder definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelSolNetworkOperation	Gewährt die Berechtigung zum Abbrechen eines Netzwerkvorgangs	Schreiben	network-operation*		
CreateSolFunctionPackage	Gewährt Berechtigungen zum Erstellen eines Funktionspakets	Schreiben	function-package*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSolNetworkInstance	Gewährt die Berechtigung zum Erstellen einer Netzwerk-Instance	Schreiben	network-instance*		
			network-package*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSolNetworkPackage	Gewährt die Berechtigung zum Erstellen eines Netzwerkpakets	Schreiben	network-package*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSolFunctionPackage	Gewährt die Berechtigung zum Löschen eines Funktionspakets	Schreiben	function-package*		
DeleteSolNetworkInstance	Gewährt die Berechtigung zum Löschen einer Netzwerk-Instance	Schreiben	network-instance*		
DeleteSolNetworkPackage	Gewährt die Berechtigung zum Löschen eines Netzwerkpakets	Schreiben	network-package*		
GetSolFunctionInstance	Gewährt die Berechtigung zum Abrufen einer Funktions-Instance	Lesen	function-instance*		
				aws:ResourceTag/${TagKey}	
GetSolFunctionPackage	Gewährt die Berechtigung zum Abrufen eines Funktionspakets	Lesen	function-package*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
GetSolFunctionPackageContent	Gewährt die Berechtigung zum Abrufen des Inhalts eines Funktionspakets	Lesen	function-package*		
				aws:ResourceTag/${TagKey}	
GetSolFunctionPackageDescriptor	Gewährt die Berechtigung zum Abrufen des Deskriptors eines Funktionspakets	Lesen	function-package*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkInstance	Gewährt die Berechtigung zum Abrufen einer Netzwerk-Instance	Lesen	network-instance*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkOperation	Gewährt die Berechtigung zum Abrufen eines Netzwerkvorgangs	Lesen	network-operation*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetSolNetworkPackage	Gewährt die Berechtigung zum Abrufen eines Netzwerkpakets	Lesen	network-package*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkPackageContent	Gewährt die Berechtigung zum Abrufen des Inhalts eines Netzwerkpakets	Lesen	network-package*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkPackageDescriptor	Gewährt die Berechtigung zum Abrufen des Deskriptors eines Netzwerkpakets	Lesen	network-package*		
				aws:ResourceTag/${TagKey}	
InstantiateSolNetworkInstance	Gewährt die Berechtigung zum Instanziieren einer Netzwerk-Instance	Schreiben	network-instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListSolFunctionInstances	Gewährt die Berechtigung zum Auflisten von Funktions-Instances	Auflisten	function-instance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
ListSolFunctionPackages	Gewährt die Berechtigung zum Auflisten von Funktionspaketen	Auflisten	function-package*		
				aws:ResourceTag/${TagKey}	
ListSolNetworkInstances	Gewährt die Berechtigung zum Auflisten von Netzwerk-Instances	Auflisten	network-instance*		
				aws:ResourceTag/${TagKey}	
ListSolNetworkOperations	Gewährt die Berechtigung zum Auflisten von Netzwerkvorgängen	Auflisten	network-operation*		
				aws:ResourceTag/${TagKey}	
ListSolNetworkPackages	Gewährt die Berechtigung zum Auflisten von Netzwerkpaketen	Auflisten	network-package*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt Berechtigungen zum Zurückgeben einer Liste der Tags für eine Ressource	Auflisten			
PutSolFunctionPackageContent	Gewährt die Berechtigung zum Hochladen des Inhalts eines Funktionspakets	Schreiben	function-package*		
PutSolNetworkPackageContent	Gewährt die Berechtigung zum Hochladen des Inhalts eines Netzwerkpakets	Schreiben	network-package*		
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zur angegebenen Ressource	Markierung	function-instance		
			function-package		
			network-instance		
			network-operation		
			network-package		
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TerminateSolNetworkInstance	Gewährt die Berechtigung zum Beenden einer Netzwerk-Instance	Schreiben	network-instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus der angegebenen Ressource	Markierung	function-instance		
			function-package		
			network-instance		
			network-operation		
			network-package		
				aws:TagKeys	
UpdateSolFunctionPackage	Gewährt die Berechtigung zum Aktualisieren eines Funktionspakets	Schreiben	function-package*		
UpdateSolNetworkInstance	Gewährt die Berechtigung zum Aktualisieren einer Netzwerk-Instance	Schreiben	function-instance*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			network-instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateSolNetworkPackage	Gewährt die Berechtigung zum Aktualisieren eines Netzwerkpakets	Schreiben	network-package*		
ValidateSolFunctionPackageContent	Gewährt die Berechtigung zum Validieren des Inhalts eines Funktionspakets	Schreiben	function-package*		
ValidateSolNetworkPackageContent	Gewährt die Berechtigung zum Validieren des Inhalts eines Netzwerkpakets	Schreiben	network-package*		

Von AWS Telco Network Builder definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
function-package	`arn:${Partition}:tnb:${Region}:${Account}:function-package/${FunctionPackageId}`	aws:ResourceTag/${TagKey}
network-package	`arn:${Partition}:tnb:${Region}:${Account}:network-package/${NetworkPackageId}`	aws:ResourceTag/${TagKey}
network-instance	`arn:${Partition}:tnb:${Region}:${Account}:network-instance/${NetworkInstanceId}`	aws:ResourceTag/${TagKey}
function-instance	`arn:${Partition}:tnb:${Region}:${Account}:function-instance/${FunctionInstanceId}`	aws:ResourceTag/${TagKey}
network-operation	`arn:${Partition}:tnb:${Region}:${Account}:network-operation/${NetworkOperationId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Telco Network Builder

AWS Telco Network Builder definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Prüfen des Vorhandenseins von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach der Prüfung von Tag-Schlüssel-Wert-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüsseln in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Textract

Amazon Textract (Servicepräfix: `textract`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Textract definierte Aktionen
- Von Amazon Textract definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Textract

Von Amazon Textract definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AnalyzeDocument	Gewährt die Berechtigung zum Erkennen von Instances	Lesen			s3:GetObject

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	von realen Dokument-Entitäten in einem als Eingabe bereitgestellten Image				
AnalyzeExpense	Gewährt die Berechtigung zum Erkennen von Instances von realen Dokument-Entitäten in einem als Eingabe bereitgestellten Image	Lesen			s3:GetObject
AnalyzeID	Gewährt die Berechtigung, relevante Informationen aus Identitätsdokumenten zu erkennen, die als Eingabe bereitgestellt werden	Lesen			s3:GetObject
CreateAdapter	Gewährt die Berechtigung zum Erstellen eines Amazon-Textract-Adapters	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAdapterVersion	Gewährt die Berechtigung zum Erstellen einer Amazon-Textract-Adapterversion	Schreiben	adapter*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteAdapter	Gewährt die Berechtigung zum Löschen eines Amazon-Textract-Adapters	Schreiben	adapter*		
DeleteAdapterVersion	Gewährt die Berechtigung zum Löschen einer Amazon-Textract-Adapterversion	Schreiben	adapterversion*		
DetectDocumentText	Gewährt die Berechtigung zum Erkennen von Text in Dokument-Images	Lesen			s3:GetObject
GetAdapter	Gewährt die Berechtigung zum Abrufen eines Amazon-Textract-Adapters	Lesen	adapter*		
GetAdapterVersion	Gewährt die Berechtigung zum Abrufen einer Amazon-Textract-Adapterversion	Lesen	adapterversion*		
GetDocumentAnalysis	Gewährt die Berechtigung, Informationen zu einem Auftrag zur Dokumentanalyse zurückzugeben	Lesen			
GetDocumentTextDetection	Gewährt die Berechtigung, Informationen zu einem Auftrag zur Texterkennung in einem Dokument zurückzugeben	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetExpenseAnalysis	Gewährt die Berechtigung zum Zurückgeben von Informationen zu einem Ausgabenanalyse-Auftrag	Lesen			
GetLendingAnalysis	Gewährt die Berechtigung zum Abrufen von Informationen auf Seitenebene über einen Kreditanalyseauftrag	Lesen			
GetLendingAnalysisSummary	Gewährt die Berechtigung zum ABrufen von zusammengefassten Informationen über einen Kreditanalyseauftrag	Lesen			
ListAdapterVersions	Gewährt die Berechtigung zum Auflisten von Amazon-Textract-Adapterversionen	Lesen			
ListAdapters	Gewährt die Berechtigung zum Auflisten von Amazon-Textract-Adaptern	Lesen			
ListTagsForResource	Gewährt die Berechtigung zum Abrufen einer Liste von Tags, die einer Ressource zugeordnet sind	Lesen	adapter		
			adapterversion		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartDocumentAnalysis	Gewährt die Berechtigung zum Starten eines asynchronen Auftrags, um Instances von realen Dokument-Entitäten in einem als Eingabe bereitgestellten Image oder PDF zu erkennen	Schreiben			s3:GetObject
StartDocumentTextDetection	Gewährt die Berechtigung zum Starten eines asynchronen Auftrags zum Erkennen von Text in Dokument-Images oder PDFs	Schreiben			s3:GetObject
StartExpenseAnalysis	Gewährt die Berechtigung zum Starten eines asynchronen Auftrags, um Rechnungen oder Belege in einem als Eingabe bereitgestellten Image oder PDF zu erkennen	Schreiben			s3:GetObject
StartLendingAnalysis	Gewährt die Berechtigung zum Starten eines asynchronen Auftrags zur Erkennung von Entitäten in einem Leihdokument, wobei ein bereitgestelltes Image oder PDF als Eingabe verwendet wird	Schreiben			s3:GetObject

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Tags zu einer Ressource	Markieren	adapter		
			adapterversion		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung, ein oder mehrere Tags aus einer Ressource zu entfernen	Markierung	adapter		
			adapterversion		
				aws:TagKeys	
UpdateAdapter	Gewährt die Berechtigung zum Aktualisieren eines Amazon-Textract-Adapters	Schreiben	adapter*		

Von Amazon Textract definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
adapter	`arn:${Partition}:textract:${Region}:${Account}:/adapters/${AdapterId}`	aws:ResourceTag/${TagKey}
adapterversion	`arn:${Partition}:textract:${Region}:${Account}:/adapters/${AdapterId}/versions/${AdapterVersion}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Textract

Amazon Textract definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch Tags, die in der Anforderung übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf Tags, die der Ressource zugeordnet sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf Tag-Schlüsseln, die in der Anforderung übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Timestream

Amazon Timestream (Servicepräfix: `timestream`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Timestream definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CancelQuery	Gewährt die Berechtigung zum Stornieren von Anfragen in Ihrem Konto	Schreiben			timestream:DescribeEndpoints
CreateBatchLoadTask	Gewährt die Berechtigung zum Erstellen einer Stapellast-Aufgabe in Ihrem Konto	Schreiben	table*		timestream:DescribeEndpoints timestream:WriteRecords

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDatabase	Gewährt die Berechtigung zum Erstellen einer Datenbank in Ihrem Konto	Schreiben	database*		timestream:DescribeEndpoints
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScheduledQuery	Gewährt die Berechtigung zum Erstellen einer geplanten Abfrage in Ihrem Konto	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole timestream:DescribeEndpoints
CreateTable	Gewährt die Berechtigung zum Erstellen einer Tabelle in Ihrem Konto	Schreiben	table*		timestream:DescribeEndpoints
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteDatabase	Gewährt die Berechtigung zum Löschen einer Datenbank in Ihrem Konto	Schreiben	database*		timestream:DescribeEndpoints
DeleteScheduledQuery	Gewährt die Berechtigung zum Löschen einer geplanten Abfrage in Ihrem Konto	Schreiben	scheduled-query*		timestream:DescribeEndpoints
DeleteTable	Gewährt die Berechtigung zum Löschen einer Tabelle in Ihrem Konto	Schreiben	table*		timestream:DescribeEndpoints
DescribeAccountSettings	Erteilt die Erlaubnis, Ihre Kontoeinstellungen zu beschreiben	Lesen			timestream:DescribeEndpoints
DescribeBatchLoadTask	Gewährt die Berechtigung zum Beschreiben einer Stapellast-Aufgabe in Ihrem Konto	Lesen			timestream:DescribeEndpoints
DescribeDatabase	Gewährt die Berechtigung zum Beschreiben einer Datenbank in Ihrem Konto	Lesen	database*		timestream:DescribeEndpoints
DescribeEndpoints	Gewährt die Berechtigung zum Beschreiben von Timestream-Endpunkten	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeScheduledQuery	Gewährt die Berechtigung zum Beschreiben einer geplanten Abfrage in Ihrem Konto	Lesen	scheduled-query*		timestream:DescribeEndpoints
DescribeTable	Gewährt die Berechtigung zum Beschreiben einer Tabelle in Ihrem Konto	Lesen	table*		timestream:DescribeEndpoints
ExecuteScheduledQuery	Gewährt die Berechtigung zum Ausführen einer geplanten Abfrage in Ihrem Konto	Schreiben	scheduled-query*		timestream:DescribeEndpoints
GetAwsBackupStatus	Gewährt die Berechtigung zum Abrufen eines Tabellenaufnahme	Lesen			timestream:DescribeEndpoints
GetAwsRestoreStatus	Gewährt die Berechtigung zum Abrufen eines Datenaufnahme	Lesen			timestream:DescribeEndpoints
ListBatchLoadTasks	Gewährt die Berechtigung zum Auflisten von Stapellast-Aufgaben in Ihrem Konto	Auflisten			timestream:DescribeEndpoints

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDatabases	Gewährt die Berechtigung zum Auflisten von Datenbanken in Ihrem Konto	Auflisten			timestream:DescribeEndpoints
ListMeasures	Gewährt die Berechtigung zum Auflisten der Kennzahlen einer Tabelle in Ihrem Konto	Auflisten	table*		timestream:DescribeEndpoints
ListScheduledQueries	Gewährt die Berechtigung zum Auflisten von geplanten Abfragen in Ihrem Konto	Auflisten			timestream:DescribeEndpoints
ListTables	Gewährt die Berechtigung zum Auflisten von Tabellen in Ihrem Konto	Auflisten	database*		timestream:DescribeEndpoints
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags einer Ressource in Ihrem Konto	Lesen	database*		timestream:DescribeEndpoints
			scheduled-query*		
			table*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PrepareQuery	Gewährt die Berechtigung zum Ausgeben von prepare-Abfragen	Lesen	table*		timestream:DescribeEndpoints timestream:Select
ResumeBatchLoadTask	Gewährt die Berechtigung zum Zusammenfassen einer Stapellast-Aufgabe in Ihrem Konto	Schreiben			timestream:DescribeEndpoints timestream:WriteRecords
Select	Gewährt die Berechtigung zum Ausgeben von „select from table“-Abfragen	Lesen	table*		timestream:DescribeEndpoints
SelectValues	Gewährt die Berechtigung zum Ausgeben von „select 1“-Abfragen	Lesen			timestream:DescribeEndpoints
StartAwsBackupJob	Gewährt die Berechtigung zum Starten eines Datenaufnahme für eine Timestream-Tabelle	Schreiben	table*		timestream:DescribeEndpoints

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartAwsRestoreJob	Gewährt die Berechtigung zum Starten der Wiederherstellungsaufgabe für ein Backup der Timestream-Tabelle	Schreiben	table*		timestream:DescribeEndpoints
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer Ressource	Tagging	database*		timestream:DescribeEndpoints
			scheduled-query*		
			table*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Unload	Gewährt die Berechtigung zum Ausgeben von Entladungs-Abfragen	Schreiben	table*		s3:AbortMultipartUpload s3:GetObject s3:PutObject timestream:DescribeEndpoints timestream:Select
UntagResource	Gewährt die Berechtigung zum Entfernen eines Tags von einer Ressource	Tagging	database*		timestream:DescribeEndpoints
			scheduled-query*		
			table*		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateAccountSettings	Erteilt die Erlaubnis, Ihre Kontoeinstellungen zu aktualisieren	Schreiben			timestream:DescribeEndpoints
UpdateDatabase	Gewährt die Berechtigung zum Aktualisieren einer Datenbank in Ihrem Konto	Schreiben	database*		timestream:DescribeEndpoints
UpdateScheduledQuery	Gewährt die Berechtigung zum Aktualisieren einer geplanten Abfrage in Ihrem Konto	Schreiben	scheduled-query*		timestream:DescribeEndpoints
UpdateTable	Gewährt die Berechtigung zum Aktualisieren einer Tabelle in Ihrem Konto	Schreiben	table*		timestream:DescribeEndpoints
WriteRecords	Gewährt die Berechtigung zur Aufnahme von Daten in eine Tabelle in Ihrem Konto	Schreiben	table*		timestream:DescribeEndpoints

Von Amazon Timestream definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
database	`arn:${Partition}:timestream:${Region}:${Account}:database/${DatabaseName}`	aws:ResourceTag/${TagKey}
table	`arn:${Partition}:timestream:${Region}:${Account}:database/${DatabaseName}/table/${TableName}`	aws:ResourceTag/${TagKey}
scheduled-query	`arn:${Partition}:timestream:${Region}:${Account}:scheduled-query/${ScheduledQueryName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Timestream

Amazon Timestream definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	String
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	String

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Timestream InfluxDB

Amazon Timestream InfluxDB (Servicepräfix: `timestream-influxdb`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Timestream InfluxDB definierte Aktionen
- Von Amazon Timestream InfluxDB definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Timestream InfluxDB

Von Amazon Timestream InfluxDB definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateDbInstance	Gewährt die Berechtigung zum Erstellen einer neuen Timestream InfluxDB-Instance	Schreiben	db-parameter-group		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDbParameterGroup	Gewährt die Berechtigung zum Erstellen einer neuen Timestream InfluxDB-Parametergruppe	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDbInstance	Gewährt die Berechtigung zum Löschen einer Timestream InfluxDB-Instance	Schreiben	db-instance*		
GetDbInstance	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Timestream InfluxDB-Instance	Lesen	db-instance*		
GetDbParameterGroup	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Timestream InfluxDB-Parametergruppe	Lesen	db-parameter-group*		
ListDbInstances	Gewährt die Berechtigung zum Auflisten von Informationen zu allen TimestreamInfluxDB-Instances im Konto	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDbParameterGroups	Gewährt die Berechtigung zum Auflisten von Informationen zu allen Timestream InfluxDB-Parametergruppen	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Timestream-InfluxDB-Ressource	Lesen		aws:ResourceTag/${TagKey}	
TagResource	Gewährt die Berechtigung zum Markieren einer Timestream InfluxDB-Ressource	Tagging	db-instance		
			db-parameter-group		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Timestream InfluxDB-Ressource	Tagging	db-instance		
			db-parameter-group		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateDbInstance	Gewährt die Berechtigung zum Aktualisieren einer Timestream InfluxDB-Instance	Schreiben	db-instance* db-parameter-group		

Von Amazon Timestream InfluxDB definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
db-instance	`arn:${Partition}:timestream-influxdb:${Region}:${Account}:db-instance/${DbInstanceIdentifier}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
db-parameter-group	`arn:${Partition}:timestream-influxdb:${Region}:${Account}:db-parameter-group/${DbParameterGroupIdentifier}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Timestream InfluxDB

Amazon Timestream InfluxDB definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wertepaaren, die in der Anforderung zulässig sind	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paar einer Ressource	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach Liste von Tag-Schlüsseln, die in der Anforderung zulässig sind	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Tiros

AWS Tiros (Servicepräfix: `tiros`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Tiros definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateQuery [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer VPC-Erreichbarkeitsabfrage	Write			
ExtendQuery [nur Berechtigung]	Erteilt die Berechtigung, eine VPC-Erreichbarkeitsabfrage auf das Konto des aufrufenden Auftraggebers zu erweitern	Schreiben			
GetQueryAnswer [nur Berechtigung]	Gewährt die Erlaubnis, Antworten auf VPC-Erreichbarkeit zu erhalten	Read			
GetQueryExplanation [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von VPC-Erreichbarkeitsabfrageerklärungen	Lesen			
GetQueryExtensionAccounts [nur Berechtigung]	Erteilt die Berechtigung, Konten aufzulisten, die in einer neuen Abfrage nützlich sein könnten	Lesen			

Von AWS Tiros definierte Ressourcentypen

AWS Tiros unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf AWS Tiros zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Tiros

Tiros besitzt keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Transcribe

Amazon Transcribe (Servicepräfix: `transcribe`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Transcribe definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateCallAnalyticsCategory	Gewährt die Berechtigung zum Erstellen einer Analysekategorie Amazon Transcribe wendet die in Ihren Analysekategorien festgeleg	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	ten Bedingungen auf Ihre Anrufanalyseaufträge an				
CreateLanguageModel	Gewährt die Berechtigung zum Erstellen eines neuen benutzerdefinierten Sprachmodells.	Write		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject s3:ListBucket
CreateMedicalVocabulary	Gewährt die Berechtigung zum Erstellen eines neuen benutzerdefinierten Vokabulars, das Sie verwenden können, um zu ändern, wie Amazon Transcribe Medical die Transkription einer Audiodatei ausführt.	Write		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
CreateVocabulary	Gewährt die Berechtigung zum Erstellen eines neuen benutzerdefinierten Vokabulars, das Sie verwenden können, um die Art zu ändern, wie Amazon Transcribe die Transkription einer Audiodatei ausführt	Write		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateVocabularyFilter	Gewährt die Berechtigung zum Erstellen eines neuen Wortschatzfilters, mit dem Sie Wörter aus der Transkription einer von Amazon Transcribe erzeugten Audiodatei herausfiltern können	Write		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
DeleteCallAnalyticsCategory	Gewährt die Berechtigung zum Löschen einer Anrufanalyse-Kategorie unter Verwendung ihres Namens aus Amazon Transcribe	Write			
DeleteCallAnalyticsJob	Gewährt die Berechtigung zum Löschen einer zuvor übermittelten Auftrags zur Anrufanalyse zusammen mit allen anderen generierten Ergebnissen, wie z. B. Transkription, Modelle usw.	Write			
DeleteLanguageModel	Gewährt die Berechtigung zum Löschen eines zuvor erstellten benutzerdefinierten Sprachmodells.	Schreiben	languagemodel*		
DeleteMedicalScribeJob	Gewährt die Berechtigung zum Löschen einer zuvor übermittelten medizinischen Scribe-Aufgabe.	Schreiben	medicalscribejob*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteMedicalTranscriptionJob	Gewährt die Berechtigung zum Löschen einer zuvor übermittelten medizinischen Transkriptionsaufgabe.	Write	medicaltranscriptionjob*		
DeleteMedicalVocabulary	Gewährt die Berechtigung zum Löschen eines medizinischen Vokabulars aus Amazon Transcribe.	Write	medicalvocabulary*		
DeleteTranscriptionJob	Gewährt die Berechtigung zum Löschen einer zuvor übermittelten Transkriptionsaufgabe zusammen mit allen anderen generierten Ergebnissen, wie z. B. Transkription, Modelle usw.	Write	transcriptionjob*		
DeleteVocabulary	Gewährt die Berechtigung zum Löschen eines Vokabulars aus Amazon Transcribe.	Write	vocabulary*		
DeleteVocabularyFilter	Gewährt die Berechtigung zum Löschen eines Vokabularfilters aus Amazon Transcribe	Write	vocabularyfilter*		
DescribeLanguageModel	Gewährt die Berechtigung, Informationen zu einem benutzerdefinierten Sprachmodell zurückzugeben.	Read	languagemodel*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetCallAnalyticsCategory	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Anrufanalyse-Kategorie	Read			
GetCallAnalyticsJob	Gewährt die Berechtigung zum Zurückgeben von Informationen über einen Auftrag zur Anrufanalyse.	Lesen			
GetMedicalScribeJob	Gewährt die Berechtigung zum Zurückgeben von Informationen zu einer medizinischen Scribe-Aufgabe.	Lesen	medicalscribejob*		
GetMedicalTranscriptionJob	Gewährt die Berechtigung zum Zurückgeben von Informationen zu einer medizinischen Transkriptionsaufgabe.	Read	medicaltranscriptionjob*		
GetMedicalVocabulary	Gewährt die Erlaubnis zum Abrufen von Informationen über ein medizinisches Vokabular	Read	medicalvocabulary*		
GetTranscriptionJob	Gewährt die Berechtigung zum Zurückgeben von Informationen über eine Transkriptionsaufgabe.	Read	transcriptionjob*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetVocabulary	Gewährt die Berechtigung zum Abrufen von Informationen über ein Vokabular.	Read	vocabulary*		
GetVocabularyFilter	Gewährt die Berechtigung zum Abrufen von Informationen über einen Vokabularfilter.	Read	vocabularyfilter*		
ListCallAnalyticsCategories	Gewährt die Berechtigung zum Auflisten von erstellten Anrufanalysekategorien	List			
ListCallAnalyticsJobs	Gewährt die Berechtigung zum Auflisten von Aufträgen zur Anrufanalyse mit dem angegebenen Status.	List			
ListLanguageModels	Gewährt die Berechtigung zum Auflisten benutzerdefinierter Sprachmodelle.	Auflisten			
ListMedicalScribeJobs	Gewährt die Berechtigung zum Auflisten medizinischer Scribe-Aufgaben mit dem angegebenen Status.	Auflisten			
ListMedicalTranscriptionJobs	Gewährt die Berechtigung zum Auflisten medizinischer Transkriptionsaufgaben mit dem angegebenen Status.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListMedicalVocabularies	Gewährt die Berechtigung zum Zurückgeben einer Liste medizinischer Vokabulare, die den angegebenen Kriterien entsprechen. Wenn keine Kriterien angegeben werden, wird die gesamte Liste der Vokabulare zurückgegeben.	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen			
ListTranscriptionJobs	Gewährt die Berechtigung zum Auflisten von Transkriptionsaufgaben mit dem angegebenen Status.	List			
ListVocabularies	Gewährt die Berechtigung zum Zurückgeben einer Liste von Vokabularen, die den angegebenen Kriterien entsprechen. Wenn keine Kriterien angegeben werden, wird die gesamte Liste der Vokabulare zurückgegeben.	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListVocabularyFilters	Gewährt die Berechtigung zum Zurückgeben einer Liste von Vokabularfiltern, die den angegebenen Kriterien entsprechen. Wenn keine Kriterien angegeben sind, werden die 5 zuletzt verwendeten Wortschatzfilter zurückgegeben.	List			
StartCallAnalyticsJob	Gewährt die Berechtigung zum Starten eines asynchronen Analyseauftrags, der nicht nur die Audioaufzeichnung eines Anrufers und Agenten transkribiert, sondern auch zusätzliche Erkenntnisse zurückgibt	Schreiben		transcribe:OutputEncryptionKMSKeyId transcribe:OutputLocation	s3:GetObject
StartCallAnalyticsStreamTranscription	Gewährt die Berechtigung zum Starten eines Protokolls, bei dem Audio an Transcribe Call Analytics und die Transkriptionsergebnisse an Ihre Anwendung gestreamt werden	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartCallAnalyticsStreamTranscriptionWebSocket	Gewährt die Berechtigung zum Starten eines WebSockets, bei dem Audio an Transcribe Call Analytics und die Transkriptionsergebnisse an Ihre Anwendung gestreamt werden	Schreiben			
StartMedicalScribeJob	Gewährt die Berechtigung zum Starten einer asynchronen Aufgabe, um Gespräche zwischen Patienten und Ärzten zu transkribieren und klinische Notizen zu transkribieren.	Schreiben		transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
StartMedicalStreamTranscription	Gewährt die Berechtigung zum Starten eines Protokolls, bei dem Audio an Transcribe Medical und die Transkriptionsergebnisse an Ihre Anwendung gestreamt werden	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartMedicalStreamTranscriptionWebSocket	Gewährt die Berechtigung zum Starten eines WebSockets, bei dem Audio an Transcribe Medical und die Transkriptionsergebnisse an Ihre Anwendung gestreamt werden	Write			
StartMedicalTranscriptionJob	Gewährt die Berechtigung zum Starten einer asynchronen Aufgabe, um medizinische Sprache in Text zu transkribieren.	Write		transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId transcribe:OutputKey aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
StartStreamTranscription	Gewährt die Berechtigung zum Starten eines bidirektionalen HTTP2-Streams, um Sprache in Echtzeit in Text zu transkribieren.	Write			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartStreamTranscriptionWebSocket	Gewährt die Berechtigung zum Starten eines Websocket-Streams zu starten, um Sprache in Echtzeit in Text zu transkribieren	Write			
StartTranscriptionJob	Gewährt die Berechtigung zum Starten einer asynchronen Aufgabe, um Sprache in Text zu transkribieren.	Schreiben		transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId transcribe:OutputKey aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit bestimmten Schlüsselwertpaaren	Markieren		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UntagResource	Gewährt die Berechtigung zum Aufheben der Kennzeichnung einer Ressource mit dem angegebenen Schlüssel	Markierung		aws:TagKeys	
UpdateCallAnalyticsCategory	Gewährt die Berechtigung zum Aktualisieren der Rufanalyse-Kategorie mit neuen Werten Die UpdateMedicalVocabulary-Produktion überschreibt alle vorhandenen Daten mit den Werten, die Sie in der Anfrage angeben.	Write			
UpdateMedicalVocabulary	Gewährt die Berechtigung zum Aktualisieren eines vorhandenen medizinischen Vokabulars mit neuen Werten. Die UpdateMedicalVocabulary-Produktion überschreibt alle vorhandenen Daten mit den Werten, die Sie in der Anfrage angeben.	Write	medicalvocabulary*		s3:GetObject
UpdateVocabulary	Gewährt die Berechtigung zum Aktualisieren eines vorhandenen Vokabulars mit neuen Werten. Die UpdateVocabulary-Produktion überschreibt alle vorhandenen Daten mit den Werten, die Sie in der Anfrage angeben.	Write	vocabulary*		s3:GetObject

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateVocabularyFilter	Gewährt die Berechtigung zum Aktualisieren eines vorhandenen Vokabularfilters mit neuen Werten. Die UpdateVocabulary-Produktion überschreibt alle vorhandenen Daten mit den Werten, die Sie in der Anfrage angeben.	Write	vocabularyfilter*		s3:GetObject

Von Amazon Transcribe definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
transcriptionjob	`arn:${Partition}:transcribe:${Region}:${Account}:transcription-job/${JobName}`	aws:ResourceTag/${TagKey}
vocabulary	`arn:${Partition}:transcribe:${Region}:${Account}:vocabulary/${VocabularyName}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
vocabularyfilter	arn:${Partition}:transcribe:${Region}:${Account}:vocabulary-filter/${VocabularyFilterName}	aws:ResourceTag/${TagKey}
languagemodel	arn:${Partition}:transcribe:${Region}:${Account}:language-model/${ModelName}	aws:ResourceTag/${TagKey}
medicaltranscriptionjob	arn:${Partition}:transcribe:${Region}:${Account}:medical-transcription-job/${JobName}	aws:ResourceTag/${TagKey}
medicalvocabulary	arn:${Partition}:transcribe:${Region}:${Account}:medical-vocabulary/${VocabularyName}	aws:ResourceTag/${TagKey}
callanalyticsjob	arn:${Partition}:transcribe:${Region}:${Account}:analytics-job/${JobName}	
callanalyticscategory	arn:${Partition}:transcribe:${Region}:${Account}:analytics-category/${CategoryName}	
medicalscribejob	arn:${Partition}:transcribe:${Region}:${Account}:medical-scribe-job/${JobName}	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Transcribe

Amazon Transcribe definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff, mit Tag-Werten, die in der Anforderung zur Ressourcenerstellung erforderlich sind	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff, mit einem Tag-Wert, der der Ressource zugeordnet sein muss	Zeichenfolge
aws:TagKeys	Filtert den Zugriff, indem verbindliche Tags in der Anforderung vorhanden sein müssen	ArrayOfString
transcribe:OutputBucketName	Filtert den Zuriff durch die Steuerung des Zugriffs basierend auf dem in der Anforderung enthaltenen Ausgabe-Bucket-Namen	Zeichenfolge
transcribe:OutputEncryptionKMSKeyId	Filtert den Zuriff durch das Steuern des Zugriffs basierend auf der in der Anforderung enthaltenen KMS-Schlüssel-ID	Zeichenfolge
transcribe:OutputKey	Filtert den Zuriff durch das Steuern des Zugriffs anhand des in der Anforderung enthaltenen Ausgabeschlüssels	Zeichenfolge
transcribe:OutputLocation	Filtert den Zugriff anhand des in der Anforderung enthaltenen Ausgabeorts	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Transfer Family

AWS Transfer Family (Dienstpräfix:`transfer`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.

- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS Transfer Family definierte Aktionen
- Von AWS Transfer Family definierte Ressourcentypen
- Bedingungsschlüssel für AWS Transfer Family

Von AWS Transfer Family definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAccess	Gewährt die Berechtigung zum Hinzufügen eines Zugriffs, der einem Server zugeordnet ist	Schreiben	server*		iam:PassRole
CreateAgreement	Erteilung der Berechtigung zum Hinzufügen einer mit einem Server verbundenen Vereinbarung	Schreiben	server*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateConnector	Erteilung der Erlaubnis zum Erstellen eines Verbinders	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateProfile	Gewährt die Berechtigung zum Erstellen einer Profilaufgabe	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	
CreateServer	Gewährt die Berechtigung zum Erstellen eines Servers	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:PassRole
CreateUser	Gewährt die Berechtigung zum Hinzufügen eines Benutzers, der einem Server zugeordnet ist	Schreiben	server*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateWorkflow	Gewährt die Berechtigung zum Erstellen eines Workflows	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteAccess	Gewährt die Berechtigung zum Löschen eines Zugriffs	Schreiben	server*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteAgreement	Erteilung der Erlaubnis zum Löschen der Vereinbarung	Schreiben	agreement*		
DeleteCertificate	Erteilung der Erlaubnis zum Löschen des Zertifikats	Schreiben	certificate*		
DeleteConnector	Erteilung der Berechtigung zum Löschen des Verbinders	Schreiben	connector*		
DeleteHostKey	Gewährt die Berechtigung zum Löschen eines Hostschlüssels, der einem Server zugeordnet ist	Schreiben	host-key*		
DeleteProfile	Erteilung der Berechtigung zum Löschen des Profils	Schreiben	profile*		
DeleteServer	Gewährt die Berechtigung zum Löschen eines Servers	Write	server*		
DeleteSshPublicKey	Gewährt die Berechtigung, einen öffentlichen SSH-Schlüssel eines Benutzers zu löschen	Write	user*		
DeleteUser	Gewährt die Berechtigung zum Löschen eines Benutzers, der einem Server zugeordnet ist	Schreiben	user*		
DeleteWorkflow	Gewährt die Berechtigung zum Löschen eines Workflows	Schreiben	workflow*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeAccess	Gewährt die Berechtigung zum Beschreiben eines Zugriffs, der einem Server zugeordnet ist	Lesen	server*		
DescribeAgreement	Erteilung der Berechtigung zur Beschreibung einer einem Server zugewiesenen Vereinbarung	Lesen	agreement*		
DescribeCertificate	Erteilung der Berechtigung zur Beschreibung eines Zertifikats	Lesen	certificate*		
DescribeConnector	Erteilung der Berechtigung zur Beschreibung eines Connectors	Lesen	connector*		
DescribeExecution	Gewährt die Berechtigung zum Beschreiben einer Ausführungen, die einem Workflow zugeordnet ist	Lesen	workflow*		
DescribeHostKey	Gewährt die Berechtigung zum Beschreiben eines Hostschlüssels, der einem Server zugeordnet ist	Lesen	host-key*		
DescribeProfile	Erteilung der Berechtigung zur Profilbeschreibung	Lesen	profile*		
DescribeSecurityPolicy	Gewährt die Berechtigung zum Beschreiben einer Sicherheitsrichtlinie	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeServer	Gewährt die Berechtigung zum Beschreiben eines Servers	Read	server*		
DescribeUser	Gewährt die Berechtigung zum Beschreiben eines Benutzers, der einem Server zugeordnet ist	Lesen	user*		
DescribeWorkflow	Gewährt die Berechtigung zum Beschreiben eines Workflows	Lesen	workflow*		
ImportCertificate	Erteilung der Berechtigung zum Hinzufügen eines Zertifikats	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	
ImportHostKey	Gewährt die Berechtigung zum Hinzufügen eines Hostschlüssels zu einem Server	Schreiben	server*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ImportSshPublicKey	Gewährt die Berechtigung, einem Benutzer einen öffentlichen SSH-Schlüssel hinzuzufügen	Schreiben	user*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAccesses	Gewährt die Berechtigung zum Auflisten von Zugriffen	Lesen	server*		
ListAgreements	Erteilung der Berechtigung zur Auflistung von Vereinbarungen	Lesen	server*		
ListCertificates	Erteilung der Berechtigung zur Auflistung von Zertifikaten	Lesen			
ListConnectors	Erteilung der Berechtigung zum Auflisten von Verbindern	Lesen			
ListExecutions	Gewährt die Berechtigung zum Auflisten von Ausführungen, die einem Workflow zugeordnet sind	Lesen	workflow*		
ListHostKeys	Gewährt die Berechtigung zum Auflisten von Hostschlüsseln, die einem Server zugeordnet sind	Lesen	server*		
ListProfiles	Gewährt die Berechtigung zum Auflisten von Startprofilen	Lesen			
ListSecurityPolicies	Gewährt die Berechtigung zum Auflisten von Sicherheitsrichtlinien	List			
ListServers	Gewährt die Berechtigung zum Auflisten von Servern	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Erteilt die Berechtigung, Stichwörter für eine AWS Transfer Family Family-Ressource aufzulisten	Lesen	agreement		
			certificate		
			connector		
			host-key		
			profile		
			server		
			user		
			workflow		
ListUsers	Gewährt die Berechtigung zum Auflisten von Benutzern, die einem Server zugeordnet sind	Auflisten	server*		
ListWorkflows	Gewährt die Berechtigung zum Auflisten von Workflows	Auflisten			
SendWorkflowStepState	Gewährt die Berechtigung zum Senden eines Rückrufs für asynchrone benutzerdefinierte Schritte	Schreiben	workflow*		
StartDirectoryListing	Erteilt die Berechtigung, mithilfe eines Connectors einen Listenvorgang auf einem Remoteserver zu initiieren	Schreiben	connector*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartFileTransfer	Gewährt die Berechtigung zum Initiieren einer Connector-Dateiübertragung	Schreiben	connector*		
StartServer	Gewährt die Berechtigung zum Starten eines Servers	Write	server*		
StopServer	Gewährt die Berechtigung zum Stoppen eines Servers	Schreiben	server*		
TagResource	Erteilt die Erlaubnis, eine AWS Transfer Family Family-Ressource zu taggen	Tagging	agreement		
			certificate		
			connector		
			host-key		
			profile		
			server		
			user		
			workflow		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TestConnection	Gewährt die Berechtigung zum Testen der Verbindung eines Konnektors mit dem Remote-Server	Schreiben	connector*		
TestIdentityProvider	Gewährt die Berechtigung, den benutzerdefinierten Identitätsanbieter eines Servers zu testen	Lesen	user*		
UntagResource	Erteilt die Erlaubnis, die Markierung einer Ressource vom Typ „ AWS Transfer Family“ aufzuheben	Tagging	agreement		
			certificate		
			connector		
			host-key		
			profile		
			server		
			user		
			workflow		
				aws:TagKeys	
UpdateAccess	Gewährt die Berechtigung zum Aktualisieren eines Zugriffs	Schreiben			iam:PassRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateAgreement	Erteilung der Berechtigung zur Aktualisierung einer Vereinbarung	Schreiben	agreement*		iam:PassRole
UpdateCertificate	Erteilung der Berechtigung zur Aktualisierung eines Zertifikats	Schreiben	certificate*		
UpdateConnector	Erteilung der Berechtigung zur Aktualisierung eines Verbinders	Schreiben	connector*		iam:PassRole
UpdateHostKey	Erteilt die Berechtigung zum Aktualisieren eines Hostschlüssels	Schreiben	host-key*		
UpdateProfile	Gewährt die Berechtigung zum Aktualisieren eines Startprofils	Schreiben	profile*		
UpdateServer	Gewährt die Berechtigung zum Aktualisieren der Konfiguration eines Servers	Write	server*		iam:PassRole
UpdateUser	Gewährt die Berechtigung zum Aktualisieren der Konfiguration eines Benutzers	Schreiben	user*		iam:PassRole

Von AWS Transfer Family definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
user	`arn:${Partition}:transfer:${Region}:${Account}:user/${ServerId}/${UserName}`	aws:ResourceTag/${TagKey}
server	`arn:${Partition}:transfer:${Region}:${Account}:server/${ServerId}`	aws:ResourceTag/${TagKey}
workflow	`arn:${Partition}:transfer:${Region}:${Account}:workflow/${WorkflowId}`	aws:ResourceTag/${TagKey}
certificate	`arn:${Partition}:transfer:${Region}:${Account}:certificate/${CertificateId}`	aws:ResourceTag/${TagKey}
connector	`arn:${Partition}:transfer:${Region}:${Account}:connector/${ConnectorId}`	aws:ResourceTag/${TagKey}
profile	`arn:${Partition}:transfer:${Region}:${Account}:profile/${ProfileId}`	aws:ResourceTag/${TagKey}
agreement	`arn:${Partition}:transfer:${Region}:${Account}:agreement/${AgreementId}`	aws:ResourceTag/${TagKey}
host-key	`arn:${Partition}:transfer:${Region}:${Account}:host-key/${ServerId}/${HostKeyId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Transfer Family

AWS Transfer Family definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die

Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Translate

Amazon Translate (Servicepräfix: `translate`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon Translate definierte Aktionen
- Von Amazon Translate definierte Ressourcentypen
- Bedingungsschlüssel für Amazon Translate

Von Amazon Translate definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateParallelData	Gewährt die Berechtigung zum Erstellen paralleler Daten	Write	parallel-data		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteParallelData	Gewährt die Berechtigung zum Löschen paralleler Daten	Write	parallel-data		
DeleteTerminology	Gewährt die Berechtigung zum Löschen einer Terminologie	Write	terminology		
DescribeTextTranslationJob	Gewährt die Berechtigung, die einer asynchronen Batch-Übersetzungsaufgabe zugeordneten Eigenschaften abzurufen	Read			
GetParallelData	Gewährt die Berechtigung zum Abrufen paralleler Daten	Read	parallel-data		
GetTerminology	Gewährt die Berechtigung zum Abrufen einer Terminologie	Read	terminology		
ImportTerminology	Gewährt die Berechtigung zum Erstellen oder Aktualisieren einer Terminologie, je nachdem, ob für den angegebenen Terminolo	Schreiben	terminology		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	gienamen eine vorhanden ist oder nicht			aws:RequestTag/${TagKey} aws:TagKeys	
ListLanguages	Erteilt die Berechtigung zum Auflisten unterstützter Sprachen	Auflisten			
ListParallelData	Gewährt die Berechtigung zum Auflisten paralleler Daten, die Ihrem Konto zugeordnet sind	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen	parallel-data terminology		
ListTerminologies	Gewährt die Berechtigung zum Auflisten von Terminologien, die Ihrem Konto zugeordnet sind	List			
ListTextTranslationJobs	Gewährt die Berechtigung zum Auflisten von Batch-Übersetzungsaufgaben, die Sie übermittelt haben	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartTextTranslationJob	Gewährt die Berechtigung zum Starten einer asynchronen Batch-Übersetzungsaufgabe. Mit Batch-Übersetzungsaufgaben können große Textmengen in mehreren Dokumenten gleichzeitig übersetzt werden.	Write	parallel-data		
			terminology		
StopTextTranslationJob	Gewährt die Berechtigung zum Beenden einer laufenden asynchronen Batch-Übersetzungsaufgabe	Schreiben			
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit bestimmten Schlüsselwertpaaren	Markierung	parallel-data		
			terminology		
				aws:RequestTag/${TagKey} aws:TagKeys	
TranslateDocument	Gewährt die Berechtigung zum Übersetzen eines Dokuments aus einer Ausgangssprache in eine Zielsprache	Lesen	terminology		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TranslateText	Gewährt die Berechtigung zum Übersetzen von Text aus einer Ausgangssprache in eine Zielsprache	Lesen	terminology		
UntagResource	Gewährt die Berechtigung zum Aufheben der Kennzeichnung einer Ressource mit dem angegebenen Schlüssel	Markierung	parallel-data		
			terminology		
				aws:TagKeys	
UpdateParallelData	Gewährt die Berechtigung zum Aktualisieren vorhandener paralleler Daten	Write	parallel-data		

Von Amazon Translate definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
terminology	`arn:${Partition}:translate:${Region}:${Account}:terminology/${ResourceName}`	aws:ResourceTag/${TagKey}
parallel-data	`arn:${Partition}:translate:${Region}:${Account}:parallel-data/${ResourceName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon Translate

Amazon Translate definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff, mit Tag-Werten, die in der Anforderung zur Ressourcenerstellung erforderlich sind	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff, mit einem Tag-Wert, der der Ressource zugeordnet sein muss	Zeichenfolge
aws:TagKeys	Filtert den Zugriff, indem verbindliche Tags in der Anforderung vorhanden sein müssen	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Trusted Advisor

AWS Trusted Advisor (Dienstpräfix:`trustedadvisor`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Trusted Advisor definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

> **Note**
>
> Die Details der IAM Trusted Advisor-Richtlinienbeschreibung gelten nur für die Trusted Advisor-Konsole. Wenn Sie den programmatischen Zugriff auf Trusted Advisor verwalten möchten, verwenden Sie die Trusted Advisor Advisor-Operationen in der AWS Support API.

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchUpdateRecommendationResourceExclusion	Erteilt die Erlaubnis, einen oder mehrere Ausschlusstatus für eine Liste von Empfehlungsressourcen zu aktualisieren	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateEngagement	Gewährt die Berechtigung zum Erstellen eines Engagements	Schreiben			
CreateEngagementAttachment	Gewährt die Berechtigung zum Erstellen eines Engagement-Anhangs	Schreiben			
CreateEngagementCommunication	Gewährt die Berechtigung zum Erstellen einer Engagement-Kommunikation	Schreiben			
DeleteNotificationConfigurationForDelegatedAdmin	Gewährt dem Organisationsverwaltungskonto die Berechtigung, E-Mail-Benachrichtigungseinstellungen aus einem delegierten Administratorkonto für Trusted Advisor Priority zu löschen	Schreiben			
DescribeAccount [nur Berechtigung]	Erteilt die Erlaubnis, den AWS Support Plan und verschiedene AWS Trusted Advisor Advisor-Einstellungen einzusehen	Lesen			
DescribeAccountAccess [nur Berechtigung]	Erteilt die Berechtigung, zu sehen, ob der AWS Trusted Advisor aktiviert oder deaktiviert AWS-Konto hat	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeCheckItems	Gewährt die Berechtigung zum Anzeigen von Details für die Prüfelemente	Lesen	checks*		
DescribeCheckRefreshStatuses	Erteilt die Berechtigung, den Aktualisierungsstatus für AWS Trusted Advisor Advisor-Prüfungen einzusehen	Lesen	checks*		
DescribeCheckStatusHistoryChanges [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen von Ergebnissen und geänderten Status für Überprüfungen der letzten 30 Tage	Lesen	checks*		
DescribeCheckSummaries	Erteilt die Berechtigung, AWS Trusted Advisor Advisor-Checkzusammenfassungen einzusehen	Lesen	checks*		
DescribeChecks	Erteilt die Erlaubnis, Details für AWS Trusted Advisor Advisor-Prüfungen einzusehen	Lesen			
DescribeNotificationConfigurations	Gewährt die Berechtigung zum Abrufen Ihrer E-Mail-Benachrichtigungseinstellungen für Trusted Advisor Priority	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeNotificationPreferences [nur Berechtigung]	Erteilt die Berechtigung zum Einsehen der Benachrichtigungseinstellungen für AWS-Konto	Lesen			
DescribeOrganization [nur Berechtigung]	Erteilt die Berechtigung zur Anzeige, ob die AWS-Konto Anforderungen zur Aktivierung der Funktion „Organisationsansicht“ erfüllt	Lesen			
DescribeOrganizationAccounts [nur Berechtigung]	Erteilt die Berechtigung zum Anzeigen der verknüpften AWS Konten in der Organisation	Lesen			
DescribeReports [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen von Details für Organisationsansichtsberichte, z. B. Berichtsname, Laufzeit, Erstellungsdatum, Status und Format.	Lesen			
DescribeRisk	Erteilt die Erlaubnis, Risikodetails in AWS Trusted Advisor Priority anzuzeigen	Lesen			
DescribeRiskResources	Erteilt die Berechtigung, die betroffenen Ressourcen für ein Risiko in AWS Trusted Advisor Priority einzusehen	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeRisks	Erteilt die Erlaubnis, Risiken in AWS Trusted Advisor Priority einzusehen	Lesen			
DescribeServiceMetadata [nur Berechtigung]	Erteilt die Berechtigung, Informationen über Berichte aus organisatorischer Sicht einzusehen AWS-Regionen, z. B. Prüfkategorien, Prüfinamen und Ressourcenstatus	Lesen			
DownloadRisk	Erteilt die Erlaubnis, eine Datei herunterzuladen, die Details zum Risiko in AWS Trusted Advisor Priority enthält	Lesen			
ExcludeCheckItems [nur Berechtigung]	Erteilt die Erlaubnis, Empfehlungen für AWS Trusted Advisor Advisor-Prüfungen auszuschließen	Schreiben	checks*		
GenerateReport [nur Berechtigung]	Erteilt die Erlaubnis, einen Bericht für AWS Trusted Advisor Advisor-Prüfungen in Ihrer Organisation zu erstellen	Schreiben			
GetEngagement	Gewährt die Berechtigung zum Anzeigen eines Engagements	Lesen			
GetEngagementAttachment	Gewährt die Berechtigung zum Anzeigen eines Engagement-Anhangs	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetEngagementType	Gewährt die Berechtigung zum Anzeigen eines bestimmten Engagement-Typs	Lesen			
GetOrganizationRecommendation	Erteilt die Erlaubnis, innerhalb der AWS Organisation einer Organisation eine bestimmte Empfehlung einzuholen. Diese API unterstützt nur priorisierte Empfehlungen	Lesen			
GetRecommendation	Gewährt die Berechtigung zum Abrufen einer spezifischen Empfehlung	Lesen			
IncludeCheckItems [nur Berechtigung]	Erteilt die Erlaubnis, Empfehlungen für AWS Trusted Advisor Advisor-Prüfungen aufzunehmen	Schreiben	checks*		
ListAccountsForParent [nur Berechtigung]	Erteilt die Berechtigung, in der Trusted Advisor Advisor-Konsole alle Konten in einer AWS Organisation anzuzeigen, die zu einem Stamm oder einer Organisationseinheit (OU) gehören	Lesen			
ListChecks	Gewährt die Berechtigung zum Auflisten von filterbaren Checks	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListEngagementCommunications	Gewährt die Berechtigung zum Anzeigen aller Mitteilungen für ein Engagement	Lesen			
ListEngagementTypes	Gewährt die Berechtigung zum Anzeigen aller Engagement-Typen	Lesen			
ListEngagements	Gewährt die Berechtigung zum Anzeigen aller Engagements	Lesen			
ListOrganizationRecommendationAccounts	Erteilt die Berechtigung, die Konten aufzulisten, denen die Ressourcen gehören, für eine Gesamtempfehlung der AWS Organisation. Diese API unterstützt nur priorisierte Empfehlungen	Auflisten			
ListOrganizationRecommendationResources	Erteilt die Berechtigung, Ressourcen einer Empfehlung innerhalb einer AWS Organisation aufzulisten. Diese API unterstützt nur priorisierte Empfehlungen	Auflisten			
ListOrganizationRecommendations	Erteilt die Berechtigung, einen filterbaren Satz von Empfehlungen innerhalb einer AWS Organisation aufzulisten. Diese API unterstützt nur priorisierte Empfehlungen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListOrganizationalUnitsForParent [nur Berechtigung]	Gewährt die Berechtigung, in der Trusted Advisor-Konsole alle Organisationseinheiten in einer übergeordneten Organisationseinheit oder einem Root-Verzeichnis anzuzeigen	Lesen			
ListRecommendationResources	Gewährt die Berechtigung zum Auflisteen von Ressourcen einer Empfehlung	Auflisten			
ListRecommendations	Gewährt die Berechtigung zum Auflisten von filterbaren Empfehlungen	Auflisten			
ListRoots [nur Berechtigung]	Erteilt die Berechtigung, in der Trusted Advisor Advisor-Konsole alle Roots anzuzeigen, die in einer AWS Organisation definiert sind	Lesen			
RefreshCheck	Erteilt die Erlaubnis, eine AWS Trusted Advisor Advisor-Überprüfung zu aktualisieren	Schreiben	checks*		
SetAccountAccess [nur Berechtigung]	Erteilt die Erlaubnis, AWS Trusted Advisor für das Konto zu aktivieren oder zu deaktivieren	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SetOrganizationAccess [nur Berechtigung]	Erteilt die Erlaubnis, die Funktion zur Organisationsansicht für AWS Trusted Advisor zu aktivieren	Schreiben			
UpdateEngagement	Gewährt die Berechtigung zum Aktualisieren der Details eines Engagements	Schreiben			
UpdateEngagementStatus	Gewährt die Berechtigung zum Aktualisieren des Status eines Engagements	Schreiben			
UpdateNotificationConfigurations	Gewährt die Berechtigung zum Erstellen oder Aktualisieren Ihrer E-Mail-Benachrichtigungseinstellungen für Trusted Advisor Priority	Schreiben			
UpdateNotificationPreferences [nur Berechtigung]	Erteilt die Erlaubnis, die Benachrichtigungseinstellungen für AWS Trusted Advisor zu aktualisieren	Schreiben			
UpdateOrganizationRecommendationLifecycle	Erteilt die Erlaubnis, den Lebenszyklus einer Empfehlung innerhalb einer AWS Organisation zu aktualisieren. Diese API unterstützt nur priorisierte Empfehlungen	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateRecommendationLifecycle	Gewährt die Berechtigung zum Aktualisieren des Lebenszyklus einer Empfehlung Diese API unterstützt nur priorisierte Empfehlungen	Schreiben			
UpdateRiskStatus	Erteilt die Erlaubnis, den Risikostatus in AWS Trusted Advisor Priority zu aktualisieren	Schreiben			

Von AWS Trusted Advisor definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

> **Note**
>
> Der ARN für den Ressourcentyp der Überprüfungen sollte keine Region enthalten. Verwenden Sie im Format statt '${Region}' ein '*', sonst wird die Richtlinie nicht richtig funktionieren.

Ressourcentypen	ARN	Bedingungsschlüssel
checks	`arn:${Partition}:trustedadvisor:${Region}:${Account}:checks/${CategoryCode}/${CheckId}`	

Bedingungsschlüssel für AWS Trusted Advisor

Trusted Advisor besitzt keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für AWS User Notifications

AWS User Notifications (Servicepräfix: `notifications`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS User Notifications definierte Aktionen
- Von AWS User Notifications definierte Ressourcentypen
- Bedingungsschlüssel für AWS User Notifications

Von AWS User Notifications definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen.

Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateChannel	Gewährt die Berechtigung, einen neuen Kanal mit einer bestimmten NotificationConfiguration zu verknüpfen	Schreiben	NotificationConfiguration*		
CreateEventRule	Gewährt die Berechtigung zum Erstellen einer neuen EventRule, wodurch diese mit einer NotificationConfiguration verbunden wird	Schreiben			
CreateNotificationConfiguration	Gewährt die Berechtigung zum Erstellen einer NotificationConfiguration	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteEventRule	Gewährt die Berechtigung zum Löschen einer EventRule	Schreiben	EventRule*		
DeleteNotificationConfiguration	Gewährt die Berechtigung zum Löschen einer NotificationConfiguration	Schreiben	NotificationConfiguration*		
DeregisterNotificationHub	Gewährt die Berechtigung zum Aufheben der Registrierung eines NotificationHub	Schreiben			
DisassociateChannel	Gewährt die Berechtigung, einen Kanal aus einer NotificationConfiguration zu entfernen	Schreiben	NotificationConfiguration*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetEventRule	Gewährt die Berechtigung zum Erhalten einer EventRule	Lesen	EventRule*		
GetNotificationConfiguration	Gewährt die Berechtigung zum Abrufen einer NotificationConfiguration	Lesen	NotificationConfiguration*		
GetNotificationEvent	Gewährt die Berechtigung zum Abrufen eines NotificationEvent	Lesen	NotificationEvent*		
ListChannels	Gewährt die Berechtigung zum Auflisten von Kanälen nach NotificationConfiguration	Auflisten			
ListEventRules	Gewährt die Berechtigung zum Auflisten von EventRules	Auflisten			
ListNotificationConfigurations	Gewährt die Berechtigung zum Auflisten von NotificationConfigurations	Auflisten			
ListNotificationEvents	Gewährt die Berechtigung zum Auflisten von NotificationEvents	Auflisten			
ListNotificationHubs	Gewährt die Berechtigung zum Auflisten von NotificationHubs	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Erhalten von Tags für eine Ressource	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RegisterNotificationHub	Gewährt die Berechtigung zum Registrieren eines NotificationHub	Schreiben			
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markierung	NotificationConfiguration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Ressource	Markierung	NotificationConfiguration*		
				aws:TagKeys	
UpdateEventRule	Gewährt die Berechtigung zum Aktualisieren einer EventRule	Schreiben	EventRule*		
UpdateNotificationConfiguration	Gewährt die Berechtigung zum Aktualisieren einer NotificationConfiguration	Schreiben	NotificationConfiguration*		

Von AWS User Notifications definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
EventRule	`arn:${Partition}:notifications::${Account}:configuration/${NotificationConfigurationId}/rule/${EventRuleId}`	
NotificationConfiguration	`arn:${Partition}:notifications::${Account}:configuration/${NotificationConfigurationId}`	aws:ResourceTag/${TagKey}
NotificationEvent	`arn:${Partition}:notifications:${Region}:${Account}:configuration/${NotificationConfigurationId}/event/${NotificationEventId}`	

Bedingungsschlüssel für AWS User Notifications

AWS User Notifications definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS User Notifications Contacts

AWS User Notifications Contacts (Servicepräfix: `notifications-contacts`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS User Notifications Contacts definierte Aktionen
- Von AWS User Notifications Contacts definierte Ressourcentypen
- Bedingungsschlüssel für AWS User Notifications Contacts

Von AWS User Notifications Contacts definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ActivateEmailContact	Gewährt die Berechtigung, den mit der angegebenen ARN verbundenen E-Mail-Kontakt zu aktivieren, wenn der angegebene Code gültig ist	Schreiben	EmailContactResource*		
CreateEmailContact	Gewährt die Berechtigung zum Erstellen eines E-Mail-Kontakts	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteEmailContact	Gewährt die Berechtigung zum Löschen eines E-Mail-Kontakts, der mit dem angegebenen ARN verbunden ist	Schreiben	EmailContactResource*		
GetEmailContact	Gewährt die Berechtigung, einen E-Mail-Kontakt zu erhalten, der mit dem angegebenen ARN verbunden ist	Lesen	EmailContactResource*		
ListEmailContacts	Gewährt die Berechtigung zum Auflisten von E-Mail-Kontakten	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Erhalten von Tags für eine Ressource	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SendActivationCode	Gewährt die Berechtigung, einen Aktivierungslink an die mit dem angegebenen ARN verbundene E-Mail zu senden	Schreiben	EmailContactResource*		
TagResource	Gewährt die Berechtigung zum Markieren einer Ressource mit Tags	Markierung	EmailContactResource*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer Ressource	Markierung	EmailContactResource*		
				aws:TagKeys	

Von AWS User Notifications Contacts definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
EmailContactResource	`arn:${Partition}:notifications-contacts::${Account}:emailcontact/${EmailContactId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS User Notifications Contacts

AWS User Notifications Contacts definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Verified Access

AWS Verified Access (Service-Präfix: `verified-access`) bietet die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Verified Access definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den

Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AllowVerifiedAccess [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer Verified Access Instance	Schreiben			

Von AWS Verified Access definierte Ressourcentypen

AWS Verified Access unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf AWS Verified Access zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für AWS Verified Access

Verified Access verfügt über keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Verified Permissions

Amazon Verified Permissions (Service-Präfix: `verifiedpermissions`) bietet die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon Verified Permissions definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateIdentitySource	Gewährt die Berechtigung zum Erstellen einer Referenz auf externen Identitätsanbieter (IDP), der mit dem OpenID Connect (OIDC)-Authentifizierungsprotokoll kompatibel ist, wie Amazon Cognito	Schreiben	policy-store*		
CreatePolicy	Gewährt die Berechtigung zum Erstellen einer Cedar-Richtlinie und diese im angegebenen Richtlinienspeicher zu speichern	Schreiben	policy-store*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreatePolicyStore	Gewährt die Berechtigung zum Erstellen einer Cedar-Richtlinie und diese im angegebenen Richtlinienspeicher zu speichern	Schreiben			
CreatePolicyTemplate	Gewährt die Berechtigung zum Erstellen einer Richtlinienvorlage	Schreiben	policy-store*		
DeleteIdentitySource	Gewährt die Berechtigung zum Löschen einer Identitätsquelle, die auf einen Identitätsanbieter (IDP) wie Amazon Cognito verweist	Schreiben	policy-store*		
DeletePolicy	Gewährt die Berechtigung zum Löschen der angegebenen Richtlinie aus dem Richtlinienspeicher	Schreiben	policy-store*		
DeletePolicyStore	Gewährt die Berechtigung zum Löschen des angegebenen Richtlinienspeichers	Schreiben	policy-store*		
DeletePolicyTemplate	Gewährt die Berechtigung zum Löschen der angegebenen Richtlinienvorlage aus dem Richtlinienspeicher	Schreiben	policy-store*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetIdentitySource	Gewährt die Berechtigung zum Abrufen der Details über die angegebene Identitätsquelle	Lesen	policy-store*		
GetPolicy	Gewährt die Berechtigung zum Abrufen von Informationen zur angegebenen Richtlinie	Lesen	policy-store*		
GetPolicyStore	Gewährt die Berechtigung zum Abrufen von Details zu einem Richtlinienspeicher	Lesen	policy-store*		
GetPolicyTemplate	Gewährt die Berechtigung zum Abrufen von Details der angegebenen Richtlinienvorlage in dem angegebenen Richtlinienspeicher	Lesen	policy-store*		
GetSchema	Gewährt die Berechtigung zum Abrufen von Details des angegebenen Schemas in dem angegebenen Richtlinienspeicher	Lesen	policy-store*		
IsAuthorized	Gewährt die Berechtigung, eine Autorisierungsentscheidung für eine in den Parametern beschriebene Serviceanfrage zu treffen	Lesen	policy-store*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
IsAuthorizedWithToken	Gewährt die Berechtigung, eine Autorisierungsentscheidung für eine in den Parametern beschriebene Serviceanfrage zu treffen. Das Prinzipal dieser Anfrage stammt aus einer externen Identitätsquelle	Lesen	policy-store*		
ListIdentitySources	Gewährt die Berechtigung zum Zurückgeben einer paginierten Liste aller Identitätsquellen, die im angegebenen Richtlinienspeicher definiert sind	Auflisten	policy-store*		
ListPolicies	Gewährt die Berechtigung zum Zurückgeben einer paginierten Liste aller Richtlinien im angegebenen Richtlinienspeicher	Auflisten	policy-store*		
ListPolicyStores	Gewährt die Berechtigung zum Zurückgeben einer paginierten Liste aller Richtlinienspeicher im aufrufenden Amazon-Web-Services-Konto	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListPolicyTemplates	Gewährt die Berechtigung zum Zurückgeben einer paginierten Liste aller Richtlinienvorlagen im angegebenen Richtlinienspeicher	Auflisten	policy-store*		
PutSchema	Gewährt die Berechtigung zum Erstellen oder Aktualisieren des Richtlinienschemas im angegebenen Richtlinienspeicher	Schreiben	policy-store*		
UpdateIdentitySource	Gewährt die Berechtigung zum Aktualisieren der angegebenen Identitätsquelle, um eine neue Identitätsanbieter (IdP)-Quelle zu verwenden, oder um die Zuordnung von Identitäten vom IdP zu einem anderen Prinzipal-Entitätstyp zu ändern	Schreiben	policy-store*		
UpdatePolicy	Gewährt die Berechtigung zum Ändern der angegebenen statischen Cedar-Richtlinie im angegebenen Richtlinienspeicher	Schreiben	policy-store*		
UpdatePolicyStore	Gewährt die Berechtigung zum Ändern der Überprüfungseinstellung für einen Richtlinienspeicher	Schreiben	policy-store*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdatePolicyTemplate	Gewährt die Berechtigung zum Aktualisieren der angegebenen Richtlinienvorlage	Schreiben	policy-store*		

Von Amazon Verified Permissions definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
policy-store	`arn:${Partition}:verifiedpermissions::${Account}:policy-store/${PolicyStoreId}`	

Bedingungsschlüssel für Amazon Verified Permissions

Verified Permissions umfasst keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon VPC Lattice

Amazon VPC Lattice (Servicepräfix: `vpc-lattice`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon VPC Lattice definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAccessLogSubscription	Gewährt die Berechtigung zum Erstellen eines neuen Zugriffsprotokollabonnements	Schreiben	AccessLogSubscription*		logs:CreateLogDelivery logs:GetLogDelivery
				aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateListener	Gewährt die Berechtigung zum Erstellen eines Listeners	Schreiben	Listener*		
				vpc-lattice:Protocol vpc-lattice:TargetGroupArns aws:TagKeys aws:RequestTag/${TagKey}	
CreateRule	Gewährt die Berechtigung zum Erstellen einer Regel.	Schreiben	Rule*		
				vpc-lattice:TargetGroupArns aws:TagKeys aws:RequestTag/${TagKey}	
CreateService	Gewährt die Berechtigung zum Erstellen eines Service	Schreiben	Service*		iam:CreateServiceLinkedRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				vpc-lattice:AuthType aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceNetwork	Gewährt die Berechtigung zum Erstellen eines Service-Netzwerks	Schreiben	ServiceNetwork*		iam:CreateServiceLinkedRole
				vpc-lattice:AuthType aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceNetworkServiceAssociation	Gewährt die Berechtigung zum Erstellen eines Service-Netzwerks und einer Service-Zuordnung	Schreiben	Service*		
			ServiceNetwork*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			ServiceNetworkServiceAssociation*		
				vpc-lattice:ServiceNetworkArn vpc-lattice:ServiceArn aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceNetworkVpcAssociation	Gewährt die Berechtigung zum Erstellen eines Service-Netzwerks und einer VPC-Zuordnung	Schreiben	ServiceNetwork*		ec2:DescribeVpcs
			ServiceNetworkVpcAssociation*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				vpc-lattice:VpcId vpc-lattice:ServiceNetworkArn vpc-lattice:SecurityGroupIds aws:TagKeys aws:RequestTag/${TagKey}	
CreateTargetGroup	Gewährt die Berechtigung zum Erstellen einer Zielgruppe	Schreiben	TargetGroup*		iam:CreateServiceLinkedRole
				vpc-lattice:VpcId aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteAccessLogSubscription	Gewährt die Berechtigung zum Löschen eines Zugriffsprotokollabonnements	Schreiben	AccessLogSubscription*		logs:DeleteLogDelivery logs:GetLogDelivery
				aws:ResourceTag/${TagKey}	
DeleteAuthPolicy	Gewährt die Berechtigung zum Löschen einer Authentifizierungsrichtlinie	Berechtigungsverwaltung	Service		
			ServiceNetwork		
DeleteListener	Gewährt die Berechtigung zum Löschen eines Listeners	Schreiben	Listener*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	Gewährt die Berechtigung zum Löschen einer Ressourcenrichtlinie	Schreiben	Service		
			ServiceNetwork		
DeleteRule	Gewährt die Berechtigung zum Löschen einer Regel	Schreiben	Rule*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteService	Gewährt die Berechtigung zum Löschen eines Service	Schreiben	Service*		
				aws:ResourceTag/${TagKey}	
DeleteServiceNetwork	Gewährt die Berechtigung zum Löschen eines Service-Netzwerks	Schreiben	ServiceNetwork*		
				aws:ResourceTag/${TagKey}	
DeleteServiceNetworkServiceAssociation	Gewährt die Berechtigung zum Löschen einer Service-Netzwerk-Zuordnung	Schreiben	ServiceNetworkServiceAssociation*		
				vpc-lattice:ServiceNetworkArn vpc-lattice:ServiceArn aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteServiceNetworkVpcAssociation	Gewährt die Berechtigung zum Löschen einer Service-Netzwerk- und VPC-Zuordnung	Schreiben	ServiceNetworkVpcAssociation*		
				vpc-lattice:VpcId vpc-lattice:ServiceNetworkArn aws:ResourceTag/${TagKey}	
DeleteTargetGroup	Gewährt die Berechtigung zum Löschen einer Zielgruppe	Schreiben	TargetGroup*		
				aws:ResourceTag/${TagKey}	
DeregisterTargets	Gewährt die Berechtigung zum Aufheben der Registrierung von Zielen aus einer Zielgruppe	Schreiben	TargetGroup*		
GetAccessLogSubscription	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Zugriffsprotokollabonnement	Lesen	AccessLogSubscription*		logs:GetLogDelivery

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
GetAuthPolicy	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Authentifizierungsrichtlinie	Lesen	Service		
			ServiceNetwork		
GetListener	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Listeners	Lesen	Listener*		
				aws:ResourceTag/${TagKey}	
GetResourcePolicy	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Ressourcenrichtlinie	Lesen	Service		
			ServiceNetwork		
GetRule	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Regel	Lesen	Rule*		
				aws:ResourceTag/${TagKey}	
GetService	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Service	Lesen	Service*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetServiceNetwork	Gewährt die Berechtigung zum Abrufen von Informationen zu einem Service-Netzwerk	Lesen	ServiceNetwork*		
				aws:ResourceTag/${TagKey}	
GetServiceNetworkServiceAssociation	Gewährt die Berechtigung zum Abrufen von Informationen über ein Service-Netzwerk und eine Service-Zuordnung	Lesen	ServiceNetworkServiceAssociation*		
				vpc-lattice:ServiceNetworkArn vpc-lattice:ServiceArn aws:ResourceTag/${TagKey}	
GetServiceNetworkVpcAssociation	Gewährt die Berechtigung zum Abrufen von Informationen über ein Service-Netzwerk und eine VPC-Zuordnung	Lesen	ServiceNetworkVpcAssociation*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				vpc-lattice:VpcId vpc-lattice:ServiceNetworkArn aws:ResourceTag/${TagKey}	
GetTargetGroup	Gewährt die Berechtigung zum Abrufen von Informationen zu einer Zielgruppe	Lesen	TargetGroup*		
				aws:ResourceTag/${TagKey}	
ListAccessLogSubscriptions	Gewährt die Berechtigung zum Auflisten von einigen oder allen Zugriffsprotokollabonnements für ein Service-Netzwerk oder einen Service	Auflisten			
ListListeners	Gewährt die Berechtigung zum Auflisten einiger oder alle Listener	Auflisten			
ListRules	Gewährt die Berechtigung zum Auflisten einiger oder aller Regeln	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListServiceNetworkServiceAssociations	Gewährt die Berechtigung zum Auflisten von einigen oder allen Service-Netzwerken und Service-Zuordnungen	Auflisten		vpc-lattice:ServiceNetworkArn vpc-lattice:ServiceArn	
ListServiceNetworkVpcAssociations	Gewährt die Berechtigung zum Auflisten von einigen oder allen Service-Netzwerk- und VPC-Zuordnungen	Auflisten		vpc-lattice:VpcId vpc-lattice:ServiceNetworkArn	
ListServiceNetworks	Gewährt die Berechtigung zum Auflisten der Service-Netzwerke, die einem Aufruferkonto gehören oder für Ihr Konto freigegeben sind	Auflisten			
ListServices	Gewährt die Berechtigung zum Auflisten der Services, die einem Aufruferkonto gehören oder für Ihr Konto freigegeben sind	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Vpc-Lattice-Ressource	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTargetGroups	Gewährt die Berechtigung zum Auflisten einer oder aller Zielgruppen	Auflisten			
ListTargets	Gewährt die Berechtigung zum Auflisten von einigen oder allen Zielen in einer Zielgruppe	Auflisten	TargetGroup*		
PutAuthPolicy	Gewährt die Berechtigung zum Erstellen oder Aktualisieren der Authentifizierungsrichtlinie für ein Service-Netzwerk oder einen Service	Berechtigungsverwaltung	Service		
			ServiceNetwork		
PutResourcePolicy	Gewährt die Berechtigung zum Erstellen einer Ressourcenrichtlinie für ein Service-Netzwerk oder einen Service	Schreiben	Service		
			ServiceNetwork		
RegisterTargets	Gewährt die Berechtigung zum Registrieren von Zielen für eine Zielgruppe	Schreiben	TargetGroup*		
TagResource	Gewährt die Berechtigung zum Markieren einer Vpc-Lattice-Ressource	Markierung	AccessLogSubscription		
			Listener		
			Rule		
			Service		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			ServiceNetwork		
			ServiceNetworkServiceAssociation		
			ServiceNetworkVpcAssociation		
			TargetGroup		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Vpc-Lattice-Ressource	Markierung	AccessLogSubscription		
			Listener		
			Rule		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			Service		
			ServiceNetwork		
			ServiceNetworkServiceAssociation		
			ServiceNetworkVpcAssociation		
			TargetGroup		
				aws:TagKeys	
UpdateAccessLogSubscription	Gewährt die Berechtigung zum Aktualisieren eines Zugriffsprotokollabonnements	Schreiben	AccessLogSubscription*		logs:GetLogDelivery logs:UpdateLogDelivery
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateListener	Gewährt die Berechtigung zum Aktualisieren eines Listeners	Schreiben	Listener*		
				vpc-lattice:TargetGroupArns aws:ResourceTag/${TagKey}	
UpdateRule	Gewährt die Berechtigung zum Aktualisieren einer Regel	Schreiben	Rule*		
				vpc-lattice:TargetGroupArns aws:ResourceTag/${TagKey}	
UpdateService	Gewährt die Berechtigung zum Aktualisieren eines Service	Schreiben	Service*		
				vpc-lattice:AuthType aws:ResourceTag/${TagKey}	
UpdateServiceNetwork	Gewährt die Berechtigung zum Aktualisieren eines Service-Netzwerks	Schreiben	ServiceNetwork*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				vpc-lattice:AuthType aws:ResourceTag/${TagKey}	
UpdateServiceNetworkVpcAssociation	Gewährt die Berechtigung zum Aktualisieren eines Service-Netzwerks und einer VPC-Zuordnung	Schreiben	ServiceNetworkVpcAssociation*		ec2:DescribeSecurityGroups ec2:DescribeVpcs
				vpc-lattice:VpcId vpc-lattice:ServiceNetworkArn vpc-lattice:SecurityGroupIds aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateTargetGroup	Gewährt die Berechtigung zum Aktualisieren einer Zielgruppe	Schreiben	TargetGroup*		
				aws:ResourceTag/${TagKey}	

Von Amazon VPC Lattice definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
ServiceNetwork	`arn:${Partition}:vpc-lattice:${Region}:${Account}:servicenetwork/${ServiceNetworkId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:AuthType
Service	`arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}`	aws:RequestTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
		aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:AuthType
ServiceNetworkVpcAssociation	arn:${Partition}:vpc-lattice:${Region}:${Account}:servicenetworkvpcassociation/${ServiceNetworkVpcAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:SecurityGroupIds vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId
ServiceNetworkServiceAssociation	arn:${Partition}:vpc-lattice:${Region}:${Account}:servicenetworkserviceassociation/${ServiceNetworkServiceAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn

Ressourcentypen	ARN	Bedingungsschlüssel
TargetGroup	arn:${Partition}:vpc-lattice:${Region}:${Account}:targetgroup/${TargetGroupId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:VpcId
Listener	arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}/listener/${ListenerId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:Protocol vpc-lattice:TargetGroupArns
Rule	arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}/listener/${ListenerId}/rule/${RuleId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:TargetGroupArns

Ressourcentypen	ARN	Bedingungsschlüssel
AccessLogSubscription	`arn:${Partition}:vpc-lattice:${Region}:${Account}:accesslogsubscription/${AccessLogSubscriptionId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Bedingungsschlüssel für Amazon VPC Lattice

Amazon VPC Lattice definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff durch das Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString
vpc-lattice:AuthType	Filtert den Zugriff nach dem in der Anforderung angegebenen Authentifizierungstyp	Zeichenfolge

Bedingungsschlüssel	Beschreibung	Typ
vpc-lattice:Protocol	Filtert den Zugriff nach den angegebenem Protokoll in der Anforderung	Zeichenfolge
vpc-lattice:SecurityGroupIds	Filtert den Zugriff nach IDs von Sicherheitsgruppen	ArrayOfString
vpc-lattice:ServiceArn	Filtert Zugriff nach der ARN eines Services	ARN
vpc-lattice:ServiceNetworkArn	Filtert den Zugriff nach der ARN eines Service-Netzwerks	ARN
vpc-lattice:TargetGroupArns	Filtert den Zugriff nach den ARNs von Zielgruppen	ArrayOfARN
vpc-lattice:VpcId	Filtert den Zugriff nach der ID einer Virtual Private Cloud (VPC)	Zeichenfolge

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon VPC Lattice Services

Amazon VPC Lattice Services (Servicepräfix: `vpc-lattice-svcs`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon VPC Lattice Services definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Connect	Erteilt die Erlaubnis, eine Verbindung zu einem VPC Lattice-Dienst herzustellen	Schreiben	TCP Service*		
				vpc-lattice-svcs:Port vpc-lattice-svcs:ServiceNetworkArn vpc-lattice-svcs:ServiceArn vpc-lattice-svcs:SourceVpc vpc-lattice-svcs:SourceVpcOwnerAccount	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Invoke	Gewährt die Berechtigung zum Aufrufen eines VPC-Lattice-Service	Schreiben	Service*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				vpc-lattice-svcs:Port vpc-lattice-svcs:ServiceNetworkArn vpc-lattice-svcs:ServiceArn vpc-lattice-svcs:SourceVpc vpc-lattice-svcs:SourceVpcOwnerAccount vpc-lattice-svcs:RequestHeader/${HeaderName} vpc-lattice-	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				svcs:RequestQueryString/${QueryStringKey}	

Von Amazon VPC Lattice Services definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
Service	`arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}/${RequestPath}`	
TCP Service	`arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}`	

Bedingungsschlüssel für Amazon VPC Lattice Services

Amazon VPC Lattice Services definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
vpc-lattice-svcs:Port	Filtert den Zugriff nach Zielport, an den die Anforderung gestellt wird	Numerischer Wert
vpc-lattice-svcs:RequestHeader/${HeaderName}	Filtert den Zugriff nach einem Header-Name-Wert-Paar in den Anforderungsheadern	String
vpc-lattice-svcs:RequestMethod	Filtert den Zugriff nach der Methode der Anfrage	String
vpc-lattice-svcs:RequestQueryString/${QueryStringKey}	Filtert den Zugriff nach den Schlüssel-Wert-Paaren der Abfragezeichenfolge in der Anforderungs-URL	ArrayOfString
vpc-lattice-svcs:ServiceArn	Filtert den Zugriff nach der ARN des Services, der die Anforderung empfängt	ARN
vpc-lattice-svcs:ServiceNetworkArn	Filtert den Zugriff nach der ARN des Service-Netzwerks, das die Anforderung empfängt	ARN
vpc-lattice-svcs:SourceVpc	Filtert den Zugriff nach der VPC, von der aus die Anfrage gestellt wird	String
vpc-lattice-svcs:S	Filtert den Zugriff durch das eigene Konto der VPC, von der aus die Anfrage gestellt wird	String

Bedingungsschlüssel	Beschreibung	Typ
ourceVpcOwnerAccount		

Aktionen, Ressourcen und Bedingungsschlüssel für AWS WAF

AWS WAF (Servicepräfix: `waf`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS WAF definierte Aktionen
- Von AWS WAF definierte Ressourcentypen
- Bedingungsschlüssel für AWS WAF

Von AWS WAF definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn

die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateByteMatchSet	Gewährt die Berechtigung zum Erstellen eines ByteMatchSet	Write	bytematchset*		
CreateGeoMatchSet	Gewährt die Berechtigung zum Erstellen eines GeoMatchSet	Write	geomatchset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateIPSet	Gewährt die Berechtigung zum Erstellen eines IPSet.	Write	ipset*		
CreateRateBasedRule	Gewährt die Berechtigung zum Erstellen einer RateBasedRule zur Begrenzung des Volume von Anforderungen von einer einzelnen IP-Adresse	Write	ratebasedrule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRegexMatchSet	Gewährt die Berechtigung zum Erstellen eines RegexMatchSet	Write	regexmatchset*		
CreateRegexPatternSet	Gewährt die Berechtigung, ein RegexPatternSet zu erstellen	Write	regexpatternset*		
CreateRule	Gewährt die Berechtigung zum Erstellen einer Regel zum Filtern von Webanforderungen	Write	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleGroup	Gewährt die Berechtigung zum Erstellen einer RuleGroup, einer Sammlung vordefinierter Regeln, die Sie in einer WebACL verwenden können	Write	rulegroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSizeConstraintSet	Gewährt die Berechtigung zum Erstellen eines SizeConstraintSet	Write	sizeconstraintset*		
CreateSqlInjectionMatchSet	Gewährt die Berechtigung zum Erstellen eines SqlInjectionMatchSet	Write	sqlinjectionmatchset*		
CreateWebACL	Gewährt die Berechtigung zum Erstellen einer WebACL, die Regeln zum Filtern von Webanforderungen enthält	Berechtigungsverwaltung	webacl*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebACLMigrationStack	Gewährt die Berechtigung zum Erstellen einer CloudFormation-Web-ACL-Vorlage in einem S3-Bucket zum Zwecke der Migration der Web-ACL von AWS WAF Classic in AWS WAF v2	Write	webacl*		s3:PutObject

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateXssMatchSet	Gewährt die Berechtigung zum Erstellen eines XssMatchSet, mit dem Sie Anforderungen erkennen, die seitenübergreifende Scripting-Angriffe enthalten	Write	xssmatchset*		
DeleteByteMatchSet	Gewährt die Berechtigung zum Löschen eines ByteMatchSet	Write	bytematchset*		
DeleteGeoMatchSet	Gewährt die Berechtigung zum Löschen eines GeoMatchSet	Write	geomatchset*		
DeleteIPSet	Gewährt die Berechtigung zum Löschen eines IPSet	Write	ipset*		
DeleteLoggingConfiguration	Gewährt die Berechtigung zum Löschen der LoggingConfiguration aus einer Web-ACL	Write	webacl*		
DeletePermissionPolicy	Gewährt die Berechtigung zum Löschen einer IAM-Richtlinie aus einer Regelgruppe	Berechtigungsverwaltung	rulegroup*		
DeleteRateBasedRule	Gewährt die Berechtigung zum Löschen einer RateBasedRule	Write	ratebasedrule*		
DeleteRegexMatchSet	Gewährt die Berechtigung zum Löschen eines RegexMatchSet	Write	regexmatchset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteRegexPatternSet	Gewährt die Berechtigung zum Löschen eines RegexPatternSet	Write	regexpatternset*		
DeleteRule	Gewährt die Berechtigung zum Löschen einer Regel	Write	rule*		
DeleteRuleGroup	Gewährt die Berechtigung zum Löschen einer RuleGroup	Write	rulegroup*		
DeleteSizeConstraintSet	Gewährt die Berechtigung zum Löschen eines SizeConstraintSet	Write	sizeconstraintset*		
DeleteSqlInjectionMatchSet	Gewährt die Berechtigung zum Löschen eines SqlInjectionMatchSet	Write	sqlinjectionmatchset*		
DeleteWebACL	Gewährt die Berechtigung zum Löschen einer WebACL	Berechtigungsverwaltung	webacl*		
DeleteXssMatchSet	Gewährt die Berechtigung zum Löschen eines XssMatchSet	Write	xssmatchset*		
GetByteMatchSet	Gewährt die Berechtigung zum Abrufen eines ByteMatchSet	Read	bytematchset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetChangeToken	Gewährt die Berechtigung zum Abrufen eines Änderungstoken zur Verwendung in Erstellungs-, Aktualisierungs- und Löschanforderungen	Read			
GetChangeTokenStatus	Gewährt die Berechtigung zum Abrufen des Status eines Änderungstoken	Read			
GetGeoMatchSet	Gewährt die Berechtigung zum Abrufen eines GeoMatchSet	Read	geomatchset*		
GetIPSet	Gewährt die Berechtigung zum Abrufen eines IPSet	Read	ipset*		
GetLoggingConfiguration	Gewährt die Berechtigung zum Abrufen einer LoggingConfiguration für eine Web-ACL	Read	webacl*		
GetPermissionPolicy	Gewährt die Berechtigung zum Abrufen einer IAM-Richtlinie für eine Regelgruppe	Read	rulegroup*		
GetRateBasedRule	Gewährt die Berechtigung zum Abrufen einer RateBased Rule	Read	ratebasedrule*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetRateBasedRuleManagedKeys	Gewährt die Berechtigung zum Abrufen des Arrays von IP-Adressen, die derzeit von einer RateBasedRule blockiert werden	Read	ratebasedrule*		
GetRegexMatchSet	Gewährt die Berechtigung zum Abrufen eines RegexMatchSet	Read	regexmatchset*		
GetRegexPatternSet	Gewährt die Berechtigung zum Abrufen eines RegexPatternSet	Read	regexpatternset*		
GetRule	Gewährt die Berechtigung zum Abrufen einer Regel	Read	rule*		
GetRuleGroup	Gewährt die Berechtigung zum Abrufen einer RuleGroup	Read	rulegroup*		
GetSampledRequests	Gewährt die Berechtigung zum Abrufen detaillierter Informationen zu einem Beispielsatz von Webanforderungen	Read	webacl		
GetSizeConstraintSet	Gewährt die Berechtigung zum Abrufen eines SizeConstraintSet	Read	sizeconstraintset*		
GetSqlInjectionMatchSet	Gewährt die Berechtigung zum Abrufen eines SqlInjectionMatchSet	Read	sqlinjectionmatchset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetWebACL	Gewährt die Berechtigung zum Abrufen einer WebACL	Read	webacl*		
GetXssMatchSet	Gewährt die Berechtigung zum Abrufen eines XssMatchSet	Read	xssmatchset*		
ListActivatedRulesInRuleGroup	Gewährt die Berechtigung zum Abrufen eines Arrays von ActivatedRule-Objekten	List			
ListByteMatchSets	Gewährt die Berechtigung zum Abrufen eines Arrays von ByteMatchSetSummary-Objekten	List			
ListGeoMatchSets	Gewährt die Berechtigung zum Abrufen eines Arrays von GeoMatchSetSummary-Objekten	List			
ListIPSets	Gewährt die Berechtigung zum Abrufen eines Arrays von IPSetSummary-Objekten	List			
ListLoggingConfigurations	Gewährt die Berechtigung zum Abrufen eines Arrays von LoggingConfiguration-Objekten	List			
ListRateBasedRules	Gewährt die Berechtigung zum Abrufen eines Arrays von RuleSummary-Objekten	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListRegexMatchSets	Gewährt die Berechtigung zum Abrufen eines Arrays von RegexMatchSetSummary-Objekten	List			
ListRegexPatternSets	Gewährt die Berechtigung zum Abrufen eines Arrays von RegexPatternSetSummary-Objekten	List			
ListRuleGroups	Gewährt die Berechtigung zum Abrufen eines Arrays von RuleGroup-Objekten	List			
ListRules	Gewährt die Berechtigung zum Abrufen eines Arrays von RuleSummary-Objekten	List			
ListSizeConstraintSets	Gewährt die Berechtigung zum Abrufen eines Arrays von SizeConstraintSetSummary-Objekten	List			
ListSqlInjectionMatchSets	Gewährt die Berechtigung zum Abrufen eines Arrays von SqlInjectionMatchSet-Objekten	List			
ListSubscribedRuleGroups	Gewährt die Berechtigung zum Abrufen eines Arrays von RuleGroup-Objekten, die Sie abonniert haben	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTagsForResource	Gewährt die Berechtigung zum Abrufen der Tags für eine Ressource	Read	ratebasedrule		
			rule		
			rulegroup		
			webacl		
ListWebACLs	Gewährt die Berechtigung zum Abrufen eines Arrays von WebACLSummary-Objekten	List			
ListXssMatchSets	Gewährt die Berechtigung zum Abrufen eines Arrays von XssMatchSet-Objekten	List			
PutLoggingConfiguration	Gewährt die Berechtigung zum Verknüpfen einer LoggingConfiguration mit einer bestimmten Web-ACL	Write	webacl*		iam:CreateServiceLinkedRole
PutPermissionPolicy	Gewährt die Berechtigung zum Anhängen einer IAM-Richtlinie an eine Regelgruppe, um die Regelgruppe zwischen Konten zu teilen	Berechtigungsverwaltung	rulegroup*		
TagResource	Gewährt die Berechtigung zum Hinzufügen eines Tags zu einer Ressource	Markieren	ratebasedrule		
			rule		
			rulegroup		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			webacl		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen eines Tags von einer Ressource	Markieren	ratebasedrule		
			rule		
			rulegroup		
			webacl		
				aws:TagKeys	
UpdateByteMatchSet	Gewährt die Berechtigung zum Einfügen oder Löschen von ByteMatchTuple-Objekten in einem ByteMatchSet	Write	bytematchset*		
UpdateGeoMatchSet	Gewährt die Berechtigung zum Einfügen oder Löschen von GeoMatchConstraint-Objekten in ein GeoMatchSet	Write	geomatchset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateIPSet	Gewährt die Berechtigung zum Einfügen oder Löschen von IPSetDescriptor-Objekten in ein IPSet	Write	ipset*		
UpdateRateBasedRule	Gewährt die Berechtigung zum Ändern einer ratenbasierten Regel	Write	ratebasedrule*		
UpdateRegexMatchSet	Gewährt die Berechtigung zum Einfügen oder Löschen von RegexMatchTuple-Objekten in einem RegexMatchSet	Write	regexmatchset*		
UpdateRegexPatternSet	Gewährt die Berechtigung zum Einfügen oder Löschen von RegexPatternStrings in ein RegexPatternSet	Write	regexpatternset*		
UpdateRule	Gewährt die Berechtigung zum Ändern einer Regel	Write	rule*		
UpdateRuleGroup	Gewährt die Berechtigung zum Einfügen oder Löschen von ActivatedRule-Objekten in einer RuleGroup	Write	rulegroup*		
UpdateSizeConstraintSet	Gewährt die Berechtigung zum Einfügen oder Löschen von SizeConstraint-Objekten in ein SizeConstraintSet	Write	sizeconstraintset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateSqlInjectionMatchSet	Gewährt die Berechtigung zum Einfügen oder Löschen von SqlInjectionMatchTuple-Objekten in ein SqlInjectionMatchSet	Write	sqlinjectionmatchset*		
UpdateWebACL	Gewährt die Berechtigung zum Einfügen oder Löschen von ActivatedRule-Objekten in einer WebACL	Berechtigungsverwaltung	webacl*		
UpdateXssMatchSet	Gewährt die Berechtigung zum Einfügen oder Löschen von XssMatchTuple-Objekten in ein XssMatchSet	Write	xssmatchset*		

Von AWS WAF definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
bytematchset	`arn:${Partition}:waf::${Account}:bytematchset/${Id}`	

Ressourcentypen	ARN	Bedingungsschlüssel
ipset	arn:${Partition}:waf::${Account}:ipset/${Id}	
ratebasedrule	arn:${Partition}:waf::${Account}:ratebasedrule/${Id}	aws:ResourceTag/${TagKey}
rule	arn:${Partition}:waf::${Account}:rule/${Id}	aws:ResourceTag/${TagKey}
sizeconstraintset	arn:${Partition}:waf::${Account}:sizeconstraintset/${Id}	
sqlinjectionmatchset	arn:${Partition}:waf::${Account}:sqlinjectionset/${Id}	
webacl	arn:${Partition}:waf::${Account}:webacl/${Id}	aws:ResourceTag/${TagKey}
xssmatchset	arn:${Partition}:waf::${Account}:xssmatchset/${Id}	
regexmatchset	arn:${Partition}:waf::${Account}:regexmatch/${Id}	
regexpatternset	arn:${Partition}:waf::${Account}:regexpatternset/${Id}	
geomatchset	arn:${Partition}:waf::${Account}:geomatchset/${Id}	
rulegroup	arn:${Partition}:waf::${Account}:regroup/${Id}	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS WAF

AWS WAF definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf den zulässigen Werten für die einzelnen Tags	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf dem Tag-Wert, der der Ressource zugeordnet ist.	Zeichenfolge
aws:TagKeys	Filtert Aktionen basierend auf den obligatorischen Tags in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS WAF Regional

AWS WAF Regional (Service-Präfix: `waf-regional`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS WAF Regional definierte Aktionen
- Von AWS WAF Regional definierte Ressourcentypen
- Bedingungsschlüssel für AWS WAF Regional

Von AWS WAF Regional definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateWebACL	Gewährt die Berechtigung zum Verknüpfen einer WebACL mit einer Ressource	Write	loadbalancer/app/*		
			webacl*		
CreateByteMatchSet	Gewährt die Berechtigung zum Erstellen eines ByteMatchSet	Write	bytematchset*		
CreateGeoMatchSet	Gewährt die Berechtigung zum Erstellen eines GeoMatchSet	Write	geomatchset*		
CreateIPSet	Gewährt die Berechtigung zum Erstellen eines IPSet.	Write	ipset*		
CreateRateBasedRule	Gewährt die Berechtigung zum Erstellen einer RateBasedRule	Write	ratebasedrule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRegexMatchSet	Gewährt die Berechtigung zum Erstellen eines RegexMatchSet	Write	regexmatchset*		
CreateRegexPatternSet	Gewährt die Berechtigung, ein RegexPatternSet zu erstellen	Write	regexpatternset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateRule	Gewährt die Berechtigung zum Erstellen einer Regel	Write	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleGroup	Gewährt die Berechtigung zum Erstellen einer RuleGroup	Write	rulegroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSizeConstraintSet	Gewährt die Berechtigung zum Erstellen eines SizeConstraintSet	Write	sizeconstraintset*		
CreateSqlInjectionMatchSet	Gewährt die Berechtigung zum Erstellen eines SqlInjectionMatchSet	Write	sqlinjectionmatchset*		
CreateWebACL	Gewährt die Berechtigung zum Erstellen einer WebACL	Berechtigungsverwaltung	webacl*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebACLMigrationStack	Gewährt die Berechtigung zum Erstellen einer CloudFormation-Web-ACL-Vorlage in einem S3-Bucket zum Zwecke der Migration der Web-ACL von AWS WAF Classic in AWS WAF v2	Write	webacl*		s3:PutObject
CreateXssMatchSet	Gewährt die Berechtigung zum Erstellen eines XssMatchSet	Write	xssmatchset*		
DeleteByteMatchSet	Gewährt die Berechtigung zum Löschen eines ByteMatchSet	Write	bytematchset*		
DeleteGeoMatchSet	Gewährt die Berechtigung zum Löschen eines GeoMatchSet	Write	geomatchset*		
DeleteIPSet	Gewährt die Berechtigung zum Löschen eines IPSet	Write	ipset*		
DeleteLoggingConfiguration	Gewährt die Berechtigung zum Löschen einer LoggingConfiguration aus einer Web-ACL	Write	webacl*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeletePermissionPolicy	Gewährt die Berechtigung zum Löschen einer IAM-Richtlinie aus einer Regelgruppe	Berechtigungsverwaltung	rulegroup*		
DeleteRateBasedRule	Gewährt die Berechtigung zum Löschen einer RateBased Rule	Write	ratebasedrule*		
DeleteRegexMatchSet	Gewährt die Berechtigung zum Löschen eines RegexMatchSet	Write	regexmatchset*		
DeleteRegexPatternSet	Gewährt die Berechtigung zum Löschen eines RegexPatternSet	Write	regexpatternset*		
DeleteRule	Gewährt die Berechtigung zum Löschen einer Regel	Write	rule*		
DeleteRuleGroup	Gewährt die Berechtigung zum Löschen einer RuleGroup	Write	rulegroup*		
DeleteSizeConstraintSet	Gewährt die Berechtigung zum Löschen eines SizeConstraintSet	Write	sizeconstraintset*		
DeleteSqlInjectionMatchSet	Gewährt die Berechtigung zum Löschen eines SqlInjectionMatchSet	Write	sqlinjectionmatchset*		
DeleteWebACL	Gewährt die Berechtigung zum Löschen einer WebACL	Berechtigungsverwaltung	webacl*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteXssMatchSet	Gewährt die Berechtigung zum Löschen eines XssMatchSet	Write	xssmatchset*		
DisassociateWebACL	Gewährt die Berechtigung zum Löschen einer Verknüpfung zwischen einer Web-ACL und einer Ressource	Write	loadbalancer/app/*		
GetByteMatchSet	Gewährt die Berechtigung zum Abrufen eines ByteMatch Set	Read	bytematchset*		
GetChangeToken	Gewährt die Berechtigung zum Abrufen eines Änderungstoken zur Verwendung in Erstellungs-, Aktualisierungs- und Löschanforderungen	Read			
GetChangeTokenStatus	Gewährt die Berechtigung zum Abrufen des Status eines Änderungstoken	Read			
GetGeoMatchSet	Gewährt die Berechtigung zum Abrufen eines GeoMatchSet	Read	geomatchset*		
GetIPSet	Gewährt die Berechtigung zum Abrufen eines IPSet	Read	ipset*		
GetLoggingConfiguration	Gewährt die Berechtigung zum Abrufen einer LoggingConfiguration	Read	webacl*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetPermissionPolicy	Gewährt die Berechtigung zum Abrufen einer IAM-Richtlinie, die an eine RuleGroup angehängt ist	Read	rulegroup*		
GetRateBasedRule	Gewährt die Berechtigung zum Abrufen einer RateBased Rule	Read	ratebasedrule*		
GetRateBasedRuleManagedKeys	Gewährt die Berechtigung zum Abrufen des Arrays von IP-Adressen, die derzeit von einer RateBasedRule blockiert werden	Read	ratebasedrule*		
GetRegexMatchSet	Gewährt die Berechtigung zum Abrufen eines RegexMatchSet	Read	regexmatchset*		
GetRegexPatternSet	Gewährt die Berechtigung zum Abrufen eines RegexPatternSet	Read	regexpatternset*		
GetRule	Gewährt die Berechtigung zum Abrufen einer Regel	Read	rule*		
GetRuleGroup	Gewährt die Berechtigung zum Abrufen einer RuleGroup	Read	rulegroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetSampledRequests	Gewährt die Berechtigung zum Abrufen detaillierter Informationen für einen Beispielsatz von Webanforderungen	Read	webacl		
GetSizeConstraintSet	Gewährt die Berechtigung zum Abrufen eines SizeConstraintSet	Read	sizeconstraintset*		
GetSqlInjectionMatchSet	Gewährt die Berechtigung zum Abrufen eines SqlInjectionMatchSet	Read	sqlinjectionmatchset*		
GetWebACL	Gewährt die Berechtigung zum Abrufen einer WebACL	Read	webacl*		
GetWebACLForResource	Gewährt die Berechtigung zum Abrufen einer WebACL, die mit einer bestimmten Ressource verknüpft ist	Read	loadbalancer/app/*		
GetXssMatchSet	Gewährt die Berechtigung zum Abrufen eines XssMatchSet	Read	xssmatchset*		
ListActivatedRulesInRuleGroup	Gewährt die Berechtigung zum Abrufen eines Arrays von ActivatedRule-Objekten	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListByteMatchSets	Gewährt die Berechtigung zum Abrufen eines Arrays von ByteMatchSetSummary-Objekten	List			
ListGeoMatchSets	Gewährt die Berechtigung zum Abrufen eines Arrays von GeoMatchSetSummary-Objekten	List			
ListIPSets	Gewährt die Berechtigung zum Abrufen eines Arrays von IPSetSummary-Objekten	List			
ListLoggingConfigurations	Gewährt die Berechtigung zum Abrufen eines Arrays von LoggingConfiguration-Objekten	List			
ListRateBasedRules	Gewährt die Berechtigung zum Abrufen eines Arrays von RuleSummary-Objekten	List			
ListRegexMatchSets	Gewährt die Berechtigung zum Abrufen eines Arrays von RegexMatchSetSummary-Objekten	List			
ListRegexPatternSets	Gewährt die Berechtigung zum Abrufen eines Arrays von RegexPatternSetSummary-Objekten	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListResourcesForWebACL	Gewährt die Berechtigung zum Abrufen eines Arrays von Ressourcen, die mit einer bestimmten WebACL verknüpft sind	List	webacl*		
ListRuleGroups	Gewährt die Berechtigung zum Abrufen eines Arrays von RuleGroup-Objekten	List			
ListRules	Gewährt die Berechtigung zum Abrufen eines Arrays von RuleSummary-Objekten	List			
ListSizeConstraintSets	Gewährt die Berechtigung zum Abrufen eines Arrays von SizeConstraintSetSummary-Objekten	List			
ListSqlInjectionMatchSets	Gewährt die Berechtigung zum Abrufen eines Arrays von SqlInjectionMatchSet-Objekten	List			
ListSubscribedRuleGroups	Gewährt die Berechtigung zum Abrufen eines Arrays von RuleGroup-Objekten, die Sie abonniert haben	List			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags für eine Ressource	Read	ratebasedrule		
			rule		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			rulegroup		
			webacl		
ListWebACLs	Gewährt die Berechtigung zum Abrufen eines Arrays von WebACLSummary-Objekten	List			
ListXssMatchSets	Gewährt die Berechtigung zum Abrufen eines Arrays von XssMatchSet-Objekten	List			
PutLoggingConfiguration	Gewährt die Berechtigung zum Zuordnen einer LoggingConfiguration mit einer Web-ACL	Write	webacl*		iam:CreateServiceLinkedRole
PutPermissionPolicy	Gewährt die Berechtigung zum Anhängen einer IAM-Richtlinie an eine bestimmte Regelgruppe, um die gemeinsame Nutzung von Regelgruppen zwischen Konten zu unterstützen	Berechtigungsverwaltung	rulegroup*		
TagResource	Gewährt die Berechtigung zum Hinzufügen eines Tags zu einer Ressource	Markieren	ratebasedrule		
			rule		
			rulegroup		
			webacl		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung zum Entfernen eines Tags von einer Ressource	Markieren	ratebasedrule		
			rule		
			rulegroup		
			webacl		
				aws:TagKeys	
UpdateByteMatchSet	Gewährt die Berechtigung zum Einfügen oder Löschen von ByteMatchTuple-Objekten in einem ByteMatchSet	Write	bytematchset*		
UpdateGeoMatchSet	Gewährt die Berechtigung zum Einfügen oder Löschen von GeoMatchConstraint-Objekten in ein GeoMatchSet	Write	geomatchset*		
UpdateIPSet	Gewährt die Berechtigung zum Einfügen oder Löschen von IPSetDescriptor-Objekten in ein IPSet	Write	ipset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateRateBasedRule	Gewährt die Berechtigung zum Einfügen oder Löschen von Prädikatobjekten in einer ratenbasierten Regel und zum Aktualisieren des RateLimit in der Regel	Write	ratebasedrule*		
UpdateRegexMatchSet	Gewährt die Berechtigung zum Einfügen oder Löschen von RegexMatchTuple-Objekten in einem RegexMatchSet	Write	regexmatchset*		
UpdateRegexPatternSet	Gewährt die Berechtigung zum Einfügen oder Löschen von RegexPatternStrings in ein RegexPatternSet	Write	regexpatternset*		
UpdateRule	Gewährt die Berechtigung zum Einfügen oder Löschen von Prädikatobjekten in einer Regel	Write	rule*		
UpdateRuleGroup	Gewährt die Berechtigung zum Einfügen oder Löschen von ActivatedRule-Objekten in einer RuleGroup	Write	rulegroup*		
UpdateSizeConstraintSet	Gewährt die Berechtigung zum Einfügen oder Löschen von SizeConstraint-Objekten in ein SizeConstraintSet	Write	sizeconstraintset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateSqlInjectionMatchSet	Gewährt die Berechtigung zum Einfügen oder Löschen von SqlInjectionMatchTuple-Objekten in ein SqlInjectionMatchSet	Write	sqlinjectionmatchset*		
UpdateWebACL	Gewährt die Berechtigung zum Einfügen oder Löschen von ActivatedRule-Objekten in einer WebACL	Berechtigungsverwaltung	webacl*		
UpdateXssMatchSet	Gewährt die Berechtigung zum Einfügen oder Löschen von XssMatchTuple-Objekten in ein XssMatchSet	Write	xssmatchset*		

Von AWS WAF Regional definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
bytematchset	`arn:${Partition}:waf-regional:${Region}:${Account}:bytematchset/${Id}`	

Ressourcentypen	ARN	Bedingungsschlüssel
ipset	arn:${Partition}:waf-regional:${Region}:${Account}:ipset/${Id}	
loadbalancer/app/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}	
ratebasedrule	arn:${Partition}:waf-regional:${Region}:${Account}:ratebasedrule/${Id}	aws:ResourceTag/${TagKey}
rule	arn:${Partition}:waf-regional:${Region}:${Account}:rule/${Id}	aws:ResourceTag/${TagKey}
sizeconstraintset	arn:${Partition}:waf-regional:${Region}:${Account}:sizeconstraintset/${Id}	
sqlinjectionmatchset	arn:${Partition}:waf-regional:${Region}:${Account}:sqlinjectionset/${Id}	
webacl	arn:${Partition}:waf-regional:${Region}:${Account}:webacl/${Id}	aws:ResourceTag/${TagKey}
xssmatchset	arn:${Partition}:waf-regional:${Region}:${Account}:xssmatchset/${Id}	
regexmatchset	arn:${Partition}:waf-regional:${Region}:${Account}:regexmatch/${Id}	
regexpatternset	arn:${Partition}:waf-regional:${Region}:${Account}:regexpatternset/${Id}	
geomatchset	arn:${Partition}:waf-regional:${Region}:${Account}:geomatchset/${Id}	

Ressourcentypen	ARN	Bedingungsschlüssel
rulegroup	`arn:${Partition}:waf-regional:${Region}:${Account}:rulegroup/${Id}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS WAF Regional

AWS WAF Regional definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf den zulässigen Werten für die einzelnen Tags	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf dem Tag-Wert, der der Ressource zugeordnet ist	Zeichenfolge
aws:TagKeys	Filtert Aktionen basierend auf den obligatorischen Tags in der Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS WAF V2

AWS WAF V2 (Servicepräfix: `wafv2`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.

- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS WAF V2 definierte Aktionen
- Von AWS WAF V2 definierte Ressourcentypen
- Bedingungsschlüssel für AWS WAF V2

Von AWS WAF V2 definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWSzu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Associate WebACL	Gewährt die Berechtigung, eine WebACL mit einer Ressource zu verknüpfen	Write	webacl*		apigateway:SetWebACL apprunner:AssociateWebAcl appsync:SetWebACL cognito-idp:AssociateWebACL ec2:AssociateVerifiedAccessInstanceWebAcl

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					elasticloadbalancing:SetWebAcl
			apigateway		
			apprunner		
			appsync		
			loadbalancer/app/		
			userpool		
			verified-access-instance		
CheckCapacity	Gewährt die Berechtigung, die Anforderungen an Web-ACL-Kapazitätseinheiten (WCU) für einen bestimmten Umfang und einen bestimmten Regelsatz zu berechnen	Lesen			
CreateAPIKey	Gewährt die Berechtigung zum Erstellen eines API-Schlüssels für die Integration der CAPTCHA-API in Ihre JavaScript Clientanwendungen	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateIPSet	Gewährt die Berechtigung zum Erstellen eines IPSet.	Schreiben	ipset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRegexPatternSet	Gewährt die Berechtigung zum Erstellen eines RegexPatternSet	Schreiben	regexpatternset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleGroup	Gewährt die Berechtigung zum Erstellen eines RuleGroup	Schreiben	rulegroup*		
			ipset		
			regexpatternset		
				aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateWebACL	Gewährt die Berechtigung zum Erstellen einer WebACL	Schreiben	webacl*		
			ipset		
			managedruleset		
			regexpatternset		
			rulegroup		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAPIKey	Gewährt Berechtigungen zum Löschen eines API-Schlüssels	Schreiben			
DeleteFirewallManagerRuleGroups	Gewährt die Berechtigung zum Löschen FirewallManagedRulesGroups aus einer WebACL, wenn nicht mehr von Firewall Manager verwaltet	Schreiben	webacl*		
DeleteIPSet	Gewährt die Berechtigung zum Löschen eines IPSet	Schreiben	ipset*		
DeleteLoggingConfiguration	Gewährt die Berechtigung zum Löschen des LoggingConfiguration aus einer WebACL	Schreiben	webacl*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				wafv2:LogScope	
DeletePermissionPolicy	Gewährt die Berechtigung zum Löschen des PermissionPolicy auf einem RuleGroup	Berechtigungsverwaltung	rulegroup*		
DeleteRegexPatternSet	Gewährt die Berechtigung zum Löschen eines RegexPatternSet	Schreiben	regexpatternset*		
DeleteRuleGroup	Gewährt die Berechtigung zum Löschen eines RuleGroup	Schreiben	rulegroup*		
DeleteWebACL	Gewährt die Berechtigung zum Löschen einer WebACL	Schreiben	webacl*		
DescribeAllManagedProducts	Gewährt die Berechtigung zum Abrufen von Produktinformationen für eine verwaltete Regelgruppe	Lesen			
DescribeManagedProductsByVendor	Gewährt die Berechtigung zum Abrufen von Produktinformationen für eine verwaltete Regelgruppe eines bestimmten Anbieters	Lesen			
DescribeManagedRuleGroup	Gewährt die Berechtigung zum Abrufen von High-Level-Informationen für eine verwaltete Regelgruppe	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateFirewallManager [nur Berechtigung]	Gewährt die Berechtigung, die Mapping von Firewall-Manager von einer WebACL aufzuheben	Schreiben	webacl*		
DisassociateWebACL	Gewährt die Berechtigung, die Verknüpfung einer WebACL mit einer Anwendungsressource zu trennen	Schreiben	apigateway		apigateway:SetWebACL apprunner:DisassociateWebAcl appsync:SetWebACL cognito-idp:DisassociateWebACL ec2:DisassociateVerifiedAccessInstanceWebAcl elasticloadbalancing:SetWebAcl

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			apprunner		
			appsync		
			loadbalancer/app/		
			userpool		
			verified-access-instance		
GenerateMobileSdkReleaseUrl	Erteilt die Berechtigung zum Generieren einer vorsignierten Download-URL für die angegebene Version des mobilen SDK	Lesen			
GetDecryptedAPIKey	Gewährt die Berechtigung zum Zurückgeben Ihres API-Schlüssels in entschlüsselter Form. Verwenden Sie dies, um die Token-Domains zu überprüfen, die Sie für den Schlüssel definiert haben.	Lesen			
GetIPSet	Gewährt die Berechtigung zum Abrufen von Details zu einem IPSet	Lesen	ipset*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetLoggingConfiguration	Gewährt die Berechtigung zum Abrufen LoggingConfiguration für eine WebACL	Lesen	webacl*		
				aws:ResourceTag/${TagKey} wafv2:LogScope	
GetManagedRuleSet	Gewährt die Berechtigung zum Abrufen von Details zu einem ManagedRuleSet	Lesen	managedruleset*		
GetMobileSdkRelease	Erteilt die Berechtigung zum Abrufen von Informationen für die angegebene mobile SDK-Version, einschließlich Versionshinweise und Tags	Lesen			
GetPermissionPolicy	Gewährt die Berechtigung zum Abrufen eines PermissionPolicy für ein RuleGroup	Lesen	rulegroup*		
GetRateBasedStatementManagedKeys	Gewährt die Berechtigung zum Abrufen der Schlüssel, die derzeit durch eine ratenbasierte Regel blockiert sind	Lesen	webacl*		
				aws:ResourceTag/${TagKey}	
GetRegexPatternSet	Gewährt die Berechtigung zum Abrufen von Details zu einem RegexPatternSet	Lesen	regexpatternset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
GetRuleGroup	Gewährt die Berechtigung zum Abrufen von Details zu einem RuleGroup	Lesen	rulegroup *		
				aws:ResourceTag/${TagKey}	
GetSampledRequests	Gewährt die Berechtigung zum Abrufen detaillierter Informationen über eine Stichprobe von Webanforderungen	Read	webacl*		
GetWebACL	Gewährt die Berechtigung zum Abrufen von Details zu einer WebACL	Read	webacl*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetWebACLForResource	Gewährt die Berechtigung zum Abrufen der WebACL, die einer Ressource zugeordnet ist	Lesen	webacl*		apprunner:DescribeWebAclForService cognito-idp:GetWebACLForResource ec2:GetVerifiedAccessInstanceWebAcl wafv2:GetWebACL
			apigateway		
			apprunner		
			appsync		
			loadbalancer/app/		
			userpool		
			verified-access-instance		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListAPIKeys	Gewährt die Berechtigung zum Abrufen einer Liste der API-Schlüssel, die Sie für den angegebenen Bereich definiert haben	Auflisten			
ListAvailableManagedRuleGroupVersions	Gewährt die Berechtigung zum Abrufen eines Arrays verwalteter Regelgruppenversionen, die für Sie verfügbar sind	Auflisten			
ListAvailableManagedRuleGroups	Gewährt die Berechtigung zum Abrufen eines Arrays von verwalteten Regelgruppen, die für Sie verfügbar sind	Auflisten			
ListIPSets	Gewährt die Berechtigung zum Abrufen eines Arrays von IP-SetSummary Objekten für die von Ihnen verwalteten IP-Sets	Auflisten			
ListLoggingConfigurations	Gewährt die Berechtigung zum Abrufen eines Arrays Ihrer LoggingConfiguration Objekte	Auflisten		wafv2:LogScope	
ListManagedRuleSets	Gewährt die Berechtigung zum Abrufen eines Arrays Ihrer ManagedRuleSet Objekte	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListMobileSdkReleases	Erteilt die Berechtigung zum Abrufen einer Liste der verfügbaren Versionen für das mobile SDK und die angegebene Geräteplattform	Auflisten			
ListRegexPatternSets	Gewährt die Berechtigung zum Abrufen eines Arrays von RegexPatternSetSummary Objekten für die von Ihnen verwalteten Regex-Mustersätze	Auflisten			
ListResourcesForWebACL	Gewährt die Berechtigung zum Abrufen eines Arrays der Amazon-Ressourcennamen (ARNs) für die Ressourcen, die mit einer Web-ACL verknüpft sind	Auflisten	webacl*		apprunner:ListAssociatedServicesForWebAcl cognito-idp:ListResourcesForWebACL ec2:DescribeVerifiedAccessInstanceWebAclAssociations
			apprunner		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			userpool		
			verified-access-instance		
ListRuleGroups	Gewährt die Berechtigung zum Abrufen eines Arrays von RuleGroupSummary Objekten für die von Ihnen verwalteten Regelgruppen	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Read	ipset		
			regexpatternset		
			rulegroup		
			webacl		
				aws:ResourceTag/${TagKey}	
ListWebACLs	Gewährt die Berechtigung zum Abrufen eines Arrays von WebACLSummary-Objekten für die von Ihnen verwalteten Web-ACLs	List			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutFirewallManagerRuleGroups [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen von FirewallManagedRulesGroups in einer WebACL	Schreiben	webacl*		
PutLoggingConfiguration	Gewährt die Berechtigung zum Aktivieren eines LoggingConfiguration, um die Protokollierung für eine Web-ACL zu starten	Schreiben	webacl*		iam:CreateServiceLinkedRole
				wafv2:LogScope wafv2:LogDestinationResource	
PutManagedRuleSetVersions	Gewährt die Berechtigung zum Erstellen einer neuen Version eines oder zum Aktualisieren einer vorhandenen Version eines ManagedRuleSet	Schreiben	managedruleset*		
			rulegroup*		
PutPermissionPolicy	Gewährt die Berechtigung zum Anhängen einer IAM-Richtlinie an eine Ressource, die zur Freigabe von Regelgruppen zwischen Konten verwendet wird	Berechtigungsverwaltung	rulegroup*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TagResource	Gewährt die Berechtigung zum Zuordnen von Tags zu einer AWS Ressource	Tagging	ipset		
			regexpatternset		
			rulegroup		
			webacl		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
				aws:ResourceTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Zuordnung von Tags zu einer - AWS Ressource	Tagging	ipset		
			regexpatternset		
			rulegroup		
			webacl		
				aws:TagKeys	
UpdateIPSet	Gewährt die Berechtigung zum Aktualisieren eines IPSet	Schreiben	ipset*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:ResourceTag/${TagKey}	
UpdateManagedRuleSetVersionExpiryDate	Gewährt die Berechtigung zum Aktualisieren des Ablaufdatums einer Version in ManagedRuleSet	Schreiben	managedruleset*		
UpdateRegexPatternSet	Gewährt die Berechtigung zum Aktualisieren eines RegexPatternSet	Schreiben	regexpatternset*		
				aws:ResourceTag/${TagKey}	
UpdateRuleGroup	Gewährt die Berechtigung zum Aktualisieren eines RuleGroup	Schreiben	rulegroup*		
			ipset		
			regexpatternset		
				aws:ResourceTag/${TagKey}	
UpdateWebACL	Gewährt die Berechtigung zum Aktualisieren einer WebACL	Schreiben	webacl*		
			ipset		
			managedruleset		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			regexpatternset		
			rulegroup		
				aws:ResourceTag/${TagKey}	

Von AWS WAF V2 definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
webacl	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/webacl/${Name}/${Id}`	aws:ResourceTag/${TagKey}
ipset	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/ipset/${Name}/${Id}`	aws:ResourceTag/${TagKey}
managedruleset	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/managedruleset/${Name}/${Id}`	

Ressourcentypen	ARN	Bedingungsschlüssel
rulegroup	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/rulegroup/${Name}/${Id}`	aws:ResourceTag/${TagKey}
regexpatternset	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/regexpatternset/${Name}/${Id}`	aws:ResourceTag/${TagKey}
loadbalancer/app/	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}`	
apigateway	`arn:${Partition}:apigateway:${Region}::/restapis/${ApiId}/stages/${StageName}`	
appsync	`arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}`	
userpool	`arn:${Partition}:cognito-idp:${Region}:${Account}:userpool/${UserPoolId}`	
apprunner	`arn:${Partition}:apprunner:${Region}:${Account}:service/${ServiceName}/${ServiceId}`	
verified-access-instance	`arn:${Partition}:ec2:${Region}:${Account}:verified-access-instance/${VerifiedAccessInstanceId}`	

Bedingungsschlüssel für AWS WAF V2

AWS WAF V2 definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen

zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den zulässigen Werten für jeden der Tags	String
aws:ResourceTag/${TagKey}	Filtert den Zugriff nach dem Tag-Wert, der der Ressource zugeordnet ist	String
aws:TagKeys	Filtert den Zugriff nach dem Vorhandensein verbindlicher Tags in der Anforderung	ArrayOfString
wafv2:LogDestinationResource	Filtert den Zugriff nach Protokollziel-ARN für die PutLoggingConfiguration API	ARN
wafv2:LogScope	Filtert den Zugriff nach Protokollbereich für die Protokollierungskonfigurations-API	String

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Well-Architected Tool

AWS Das Well-Architected Tool (Dienstpräfix:`wellarchitected`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.

- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von AWS Well-Architected Tool definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Associate Lenses	Gewährt die Berechtigung, dem angegebenen Workload eine Linse zuzuordnen	Schreiben	workload*		
Associate Profiles	Gewährt die Berechtigung, dem angegebenen Workload ein Profil zuzuordnen	Schreiben	workload*		
Configure Integration [nur Berechtigung]	Erteilt die Berechtigung zur Konfiguration der Integration	Schreiben			
CreateLensShare	Erteilt einem Besitzer eines Objektivs die Erlaubnis, es mit anderen AWS Konten und IAM-Benutzern zu teilen	Schreiben	lens*		
CreateLensVersion	Gewährt die Berechtigung zum Erstellen einer neuen Linsenversion	Schreiben	lens*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateMilestone	Gewährt die Berechtigung zum Erstellen eines neuen Meilensteins für den angegebenen Workload	Schreiben	workload*		
CreateProfile	Gewährt die Berechtigung zum Erstellen eines neuen Profils	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfileShare	Erteilt einem Besitzer eines Profils die Erlaubnis, es mit anderen AWS Konten und IAM-Benutzern zu teilen	Schreiben	profile*		
CreateReviewTemplate	Gewährt die Berechtigung zum Erstellen einer neuen Bewertungsvorlage	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTemplateShare	Erteilt einem Besitzer einer Bewertungsvorlage die Erlaubnis, sie mit anderen AWS Konten und IAM-Benutzern zu teilen	Schreiben	review-template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateWorkload	Gewährt die Berechtigung zum Erstellen eines neuen Workloads	Write		aws:RequestTag/${TagKey} aws:TagKeys wellarchitected:JiraProjectKey	
CreateWorkloadShare	Gewährt die Berechtigung, einen Workload für ein anderes Konto freizugeben	Schreiben	workload*		
DeleteLens	Gewährt die Berechtigung zum Löschen einer Linse	Schreiben	lens*		
DeleteLensShare	Gewährt die Berechtigung zum Löschen einer bestehenden Linsen-Freigabe	Schreiben	lens*		
DeleteProfile	Gewährt die Berechtigung zum Löschen eines Profils	Schreiben	profile*		
DeleteProfileShare	Gewährt die Berechtigung zum Löschen einer bestehenden Profilfreigabe	Schreiben	profile*		
DeleteReviewTemplate	Gewährt die Berechtigung zum Löschen einer bestehenden Bewertungsvorlage	Schreiben	review-template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteTemplateShare	Gewährt die Berechtigung zum Löschen einer bestehenden Bewertungsvorlagen freigabe	Schreiben	review-template*		
DeleteWorkload	Gewährt die Berechtigung zum Löschen eines vorhandenen Workloads	Write	workload*		
DeleteWorkloadShare	Gewährt die Berechtigung zum Löschen einer bestehenden Workload-Freigabe	Write	workload*		
DisassociateLenses	Gewährt die Berechtigung, die Mapping einer Linse zum angegebenen Workload aufzuheben	Schreiben	workload*		
DisassociateProfiles	Gewährt die Berechtigung, eines Profils zum angegebenen Workload aufzuheben	Schreiben	workload*		
ExportLens	Gewährt die Berechtigung zum Löschen einer bestehenden Linse	Lesen	lens*		
GetAnswer	Gewährt die Berechtigung, die angegebene Antwort aus der angegebenen Linsenprüfung abzurufen	Lesen	workload*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetConsolidatedReport	Gewährt die Berechtigung zum Abrufen von Metriken des konsolidierten Berichts oder zum Generieren der PDF-Datei des konsolidierten Berichts in diesem Konto	Lesen			
GetGlobalSettings	Erteilt die Erlaubnis, alle Einstellungen für das Konto abzurufen	Lesen			
GetLens	Gewährt die Berechtigung zum Abrufen einer bestehenden Linse	Lesen	lens*		
				aws:ResourceTag/${TagKey}	
GetLensReview	Gewährt die Berechtigung, die angegebene Linsenprüfung des angegebenen Workloads abzurufen	Read	workload*		
GetLensReviewReport	Gewährt die Berechtigung zum Abrufen des Berichts für die angegebene Linsenprüfung	Read	workload*		
GetLensVersionDifference	Gewährt die Berechtigung, den Unterschied zwischen der angegebenen Linsenversion und der neuesten verfügbaren Linsenversion abzurufen	Read	lens*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetMilestone	Gewährt die Berechtigung zum Abrufen des angegebenen Meilensteins des angegebenen Workloads	Lesen	workload*		
GetProfile	Gewährt die Berechtigung zum Abrufen des angegebenen Profils	Lesen	profile*		
				aws:ResourceTag/${TagKey}	
GetProfileTemplate	Gewährt die Berechtigung zum Abrufen der angegebenen Profilvorlage	Lesen			
GetReviewTemplate	Gewährt die Berechtigung zum Abrufen der angegebenen Bewertungsvorlage	Lesen	review-template*		
				aws:ResourceTag/${TagKey}	
GetReviewTemplateAnswer	Gewährt die Berechtigung zum Abrufen der angegebenen Antwort aus der angegebenen Bewertungsvorlage	Lesen	review-template*		
GetReviewTemplateLensReview	Gewährt die Berechtigung zum Abrufen der angegebenen Linsenbewertung der angegebenen Bewertungsvorlage	Lesen	review-template*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetWorkload	Gewährt die Berechtigung zum Abrufen des angegebenen Workloads	Lesen	workload*		
				aws:ResourceTag/${TagKey}	
ImportLens	Gewährt die Berechtigung zum Importieren einer neuen Linse	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
ListAnswers	Gewährt die Berechtigung zum Auflisten der Antworten aus der angegebenen Linsenprüfung	Auflisten	workload*		
ListCheckDetails	Gewährt die Berechtigung zum Auflisten der Überprüfungs-Freigaben des Workloads	Auflisten	workload*		
ListCheckSummaries	Gewährt die Berechtigung zum Auflisten der Workload-Freigaben des Workloads	Auflisten	workload*		
ListLensReviewImprovements	Gewährt die Berechtigung zum Auflisten der Verbesserungen der angegebenen Linsenprüfung	List	workload*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListLensReviews	Gewährt die Berechtigung zum Auflisten der Linsenprüfungen der angegebenen Workload	Auflisten	workload*		
ListLensShares	Gewährt die Berechtigung zum Auflisten aller für eine Linse erstellten Freigaben	Auflisten	lens*		
ListLenses	Gewährt die Berechtigung zum Auflisten der für dieses Konto verfügbaren Linsen	List			
ListMilestones	Gewährt die Berechtigung zum Auflisten der Meilensteine des angegebenen Workloads	List	workload*		
ListNotifications	Gewährt die Berechtigung zum Auflisten von Benachrichtigungen im Zusammenhang mit dem Konto oder der angegebenen Ressource	Auflisten			
ListProfileNotifications	Gewährt die Berechtigung zum Auflisten von Profilbenachrichtigungen im Zusammenhang mit angegebenen Ressourcen	Auflisten			
ListProfileShares	Gewährt die Berechtigung zum Auflisten aller für ein Profil erstellten Freigaben	Auflisten	profile*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListProfiles	Gewährt die Berechtigung zum Auflisten der für dieses Konto verfügbaren Profile	Auflisten			
ListReviewTemplateAnswers	Gewährt die Berechtigung zum Auflisten der Antworten aus der angegebenen Bewertungsvorlage	Auflisten	review-template*		
ListReviewTemplates	Gewährt die Berechtigung zum Auflisten der für dieses Konto verfügbaren Bewertungsvorlagen	Auflisten			
ListShareInvitations	Gewährt die Berechtigung zum Auflisten der Workload-Freigabe-Einladungen des angegebenen Kontos oder Benutzers	List			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Well-Architected-Ressource	Lesen	lens		
			profile		
			review-template		
			workload		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListTemplateShares	Gewährt die Berechtigung zum Auflisten aller für eine Bewertungsvorlage erstellten Freigaben	Auflisten	review-template*		
ListWorkloadShares	Gewährt die Berechtigung zum Auflisten der Workload-Freigaben des angegebenen Workloads	List	workload*		
ListWorkloads	Gewährt die Berechtigung zum Auflisten der Workloads in diesem Konto	List			
TagResource	Gewährt die Berechtigung zum Markieren einer Well-Architected-Ressource	Markieren	lens		
			profile		
			review-template		
			workload		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Aufheben der Markierung einer Well-Architected-Ressource	Markieren	lens		
			profile		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			review-template		
			workload		
				aws:TagKeys	
UpdateAnswer	Gewährt die Berechtigung zum Aktualisieren der Eigenschaften der angegebenen Antwort	Schreiben	workload*		
UpdateGlobalSettings	Erteilt die Erlaubnis, alle Einstellungen für das Konto zu verwalten	Schreiben		wellarchitected:JiraProjectKey	
UpdateIntegration	Erteilt die Berechtigung, die Eigenschaften der Integration zu aktualisieren	Schreiben	workload*		
UpdateLensReview	Gewährt die Berechtigung zum Aktualisieren der Eigenschaften der angegebenen Linsenprüfung	Schreiben	workload*		
UpdateProfile	Gewährt die Berechtigung zum Aktualisieren der Eigenschaften des angegebenen Profils	Schreiben	profile*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateReviewTemplate	Gewährt die Berechtigung zum Aktualisieren der Eigenschaften der angegebenen Bewertungsvorlage	Schreiben	review-template*		
UpdateReviewTemplateAnswer	Gewährt die Berechtigung zum Aktualisieren der Eigenschaften der Antwort der angegebenen Bewertungsvorlage	Schreiben	review-template*		
UpdateReviewTemplateLensReview	Gewährt die Berechtigung zum Aktualisieren der Eigenschaften der Linsenbewertung der angegebenen Bewertungsvorlage	Schreiben	review-template*		
UpdateShareInvitation	Gewährt die Berechtigung zum Aktualisieren des Status der angegebenen Workload-Freigabe-Einladung	Write			
UpdateWorkload	Gewährt die Berechtigung zum Aktualisieren der Eigenschaften des angegebenen Workloads	Schreiben	workload*		
				wellarchitected:JiraProjectKey	
UpdateWorkloadShare	Erteilt die Berechtigung zum Aktualisieren der Eigenschaften des angegebenen Workload-Shares	Schreiben	workload*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpgradeLensReview	Gewährt die Berechtigung, ein Upgrade für die angegebene Linsenprüfung durchzuführen, um die neueste Version der zugehörigen Linse zu verwenden	Schreiben	workload*		
UpgradeProfileVersion	Gewährt die Berechtigung, ein Upgrade für den angegebenen Workload durchzuführen, um die neueste Version des zugehörigen Profils zu verwenden	Schreiben	profile* workload*		
UpgradeReviewTemplateLensReview	Gewährt die Berechtigung zum Hochstufen der angegebenen Linsenbewertung der angegebenen Bewertungsvorlage	Schreiben	review-template*		

Von AWS Well-Architected Tool definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
workload	`arn:${Partition}:wellarchitected:${Region}:${Account}:workload/${ResourceId}`	aws:ResourceTag/${TagKey}
lens	`arn:${Partition}:wellarchitected:${Region}:${Account}:lens/${ResourceId}`	aws:ResourceTag/${TagKey}
profile	`arn:${Partition}:wellarchitected:${Region}:${Account}:profile/${ResourceId}`	aws:ResourceTag/${TagKey}
review-template	`arn:${Partition}:wellarchitected:${Region}:${Account}:review-template/${ResourceId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Well-Architected Tool

AWS Das Well-Architected Tool definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach Tag-Schlüssel-Wert-Paaren in der Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüssel-Werte-Paaren, die der Ressource angefügt sind	String

Bedingungsschlüssel	Beschreibung	Typ
aws:TagKeys	Filtert Aktionen nach den Tag-Schlüsseln in der Anforderung	ArrayOfString
wellarchitected:JiraProjectKey	Filtert den Zugriff nach Projektschlüssel	String

Aktionen, Ressourcen und Bedingungsschlüssel für AWS Wickr

AWS Wickr (Service-Präfix: `wickr`) bietet die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Durch AWS Wickr definierte Aktionen
- Von AWS Wickr definierte Ressourcentypen
- Bedingungsschlüssel für AWS Wickr

Durch AWS Wickr definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateAdminSession	Gewährt die Berechtigung zum Erstellen und Verwalten von Wickr-Netzwerken	Schreiben	network*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateNetwork	Gewährt die Berechtigung zum Erstellen eines neuen Wickr-Netzwerks	Schreiben			
ListNetworks	Gewährt die Berechtigung zum Anzeigen von Wickr-Netzwerken	Schreiben			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten der Tags, die auf eine Wickr-Ressource angewendet wurden	Lesen			
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer bestimmten Wickr-Ressource	Markierung	network*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen der angegebenen Tags aus der angegebenen Wickr-Ressource	Markierung	network*		
				aws:TagKeys	
UpdateNetworkDetails	Gewährt die Berechtigung zum Aktualisieren von Wickr-Netzwerkdetails	Schreiben	network*		

Von AWS Wickr definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
network	`arn:${Partition}:wickr:${Region}:${Account}:network/${NetworkId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS Wickr

AWS Wickr definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach dem Schlüssel eines Tags und den Wert einer Anforderung	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüsselwertpaaren, die der Ressource angefügt sind	Zeichenfolge
aws:TagKeys	Filtert den Zugriff nach den Tag-Schlüsseln in einer Anforderung	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon WorkDocs

Amazon WorkDocs (Service-Präfix:`workdocs`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon definierte Aktionen WorkDocs

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AbortDocumentVersionUpload	Erteilt die Genehmigung, den Upload der angegebenen Dokumentversion abzubrechen, der zuvor initiiert wurde von InitiateDocumentVersionUpload	Schreiben			
ActivateUser	Gewährt die Berechtigung zum Aktivieren des angegebenen Benutzers Nur aktive Benutzer können auf Amazon zugreifen WorkDocs	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AddNotificationPermissions [nur Berechtigung]	Erteilt die Erlaubnis, Principals hinzuzufügen, die Abonnement-APIs für Benachrichtigungen für eine bestimmte WorkDocs Site aufrufen dürfen	Schreiben			
AddResourcePermissions	Gewährt die Berechtigung zum Erstellen einer Reihe von Berechtigungen für den angegebenen Ordner oder das angegebene Dokument	Schreiben			
AddUserToGroup [nur Berechtigung]	Gewährt die Berechtigung zum Hinzufügen eines Benutzers zu einer Gruppe	Schreiben			
CheckAlias [nur Berechtigung]	Gewährt die Berechtigung zum Überprüfen eines Alias	Lesen			
CreateComment	Gewährt die Berechtigung zum Hinzufügen eines neuen Kommentars zur angegebenen Dokumentversion	Schreiben			
CreateCustomMetadata	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer benutzerdefinierter Eigenschaften zur angegebenen Ressource	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateFolder	Gewährt die Berechtigung zum Erstellen eines Ordners mit dem angegebenen Namen und dem übergeordneten Ordner	Schreiben			
CreateInstance [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer Instance	Schreiben			
CreateLabels	Gewährt die Berechtigung zum Hinzufügen von Kennzeichnungen zu der angegebenen Ressource	Schreiben			
CreateNotification Subscription	Erteilt die Berechtigung WorkDocs zur Konfiguration für die Verwendung von Amazon SNS SNS-Benachrichtigungen	Schreiben			
CreateUser	Gewährt die Berechtigung zum Erstellen eines Benutzers in einem Simple AD- oder Microsoft AD-Verzeichnis	Schreiben			
DeactivateUser	Erteilt die Erlaubnis, den angegebenen Benutzer zu deaktivieren, wodurch dem Benutzer der Zugriff auf Amazon entzogen wird WorkDocs	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteComment	Gewährt die Berechtigung zum Löschen des angegebenen Kommentars aus der Dokumentversion	Schreiben			
DeleteCustomMetadata	Gewährt die Berechtigung zum Löschen von benutzerdefinierten Metadaten aus der angegebenen Ressource	Schreiben			
DeleteDocument	Gewährt die Berechtigung zum dauerhaften Löschen des angegebenen Dokuments und der zugehörigen Metadaten	Schreiben			
DeleteDocumentVersion	Gewährt die Berechtigung zum Löschen der Versionen eines angegebenen Dokuments	Schreiben			
DeleteFolder	Gewährt die Berechtigung zum dauerhaften Löschen des angegebenen Ordners und der zugehörigen Inhalte	Schreiben			
DeleteFolderContents	Gewährt die Berechtigung zum Löschen des Inhalts des angegebenen Ordners	Schreiben			
DeleteInstance [nur Berechtigung]	Gewährt die Berechtigung zum Löschen einer Instance	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteLabels	Gewährt die Berechtigung zum Löschen einer oder mehrerer Kennzeichnungen aus einer Ressource	Schreiben			
DeleteNotification Permissions [nur Berechtigung]	Erteilt die Erlaubnis, Principals zu löschen, die Abonnement-APIs für Benachrichtigungen für eine bestimmte Site aufrufen dürfen WorkDocs	Schreiben			
DeleteNotification Subscription	Gewährt die Berechtigung zum Löschen des angegebenen Abonnements aus der angegebenen Organisation	Schreiben			
DeleteUser	Gewährt die Berechtigung zum Löschen des angegebenen Benutzers aus einem Simple AD- oder Microsoft AD-Verzeichnis	Schreiben			
DeregisterDirectory [nur Berechtigung]	Gewährt die Berechtigung zum Aufheben der Registrierung eines Verzeichnisses	Schreiben			
DescribeActivities	Gewährt die Berechtigung zum Abrufen der Benutzeraktivitäten in einem angegebenen Zeitraum	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeAvailableDirectories [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben der verfügbaren Verzeichnisse	Auflisten			
DescribeComments	Gewährt die Berechtigung zum Auflisten aller Kommentare für die angegebene Dokumentversion	Auflisten			
DescribeDocumentVersions	Gewährt die Berechtigung zum Abrufen der Dokumentversionen für das angegebene Dokument	Auflisten			
DescribeFolderContents	Gewährt die Berechtigung zum Beschreiben der Inhalte des angegebenen Ordners, einschließlich seiner Dokumente und Unterordner	Auflisten			
DescribeGroups	Gewährt die Berechtigung zum Beschreiben der Benutzergruppen	Auflisten			
DescribeInstanceExports [nur Berechtigung]	Erteilt die Berechtigung, den Exportverlauf für eine Instanz zu beschreiben	Auflisten			
DescribeInstances [nur Berechtigung]	Gewährt die Berechtigung zum Beschreiben von Instances	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeNotificationPermissions [nur Berechtigung]	Erteilt die Erlaubnis, Principals zu beschreiben, die Abonnement-APIs für Benachrichtigungen für eine bestimmte WorkDocs Site aufrufen dürfen	Auflisten			
DescribeNotificationSubscriptions	Gewährt die Berechtigung zum Auflisten der angegebenen Benachrichtigungsabonnements	Auflisten			
DescribeResourcePermissions	Gewährt die Berechtigung zum Anzeigen einer Beschreibung der Berechtigungen einer bestimmten Ressource	Auflisten			
DescribeRootFolders	Gewährt die Berechtigung zum Beschreiben der Root-Ordner	Auflisten			
DescribeUsers	Gewährt die Berechtigung zum Anzeigen einer Beschreibung der angegebenen Benutzer Sie können alle Benutzer beschreiben oder die Ergebnisse filtern (z. B. nach Status oder Organisation).	Auflisten			
DownloadDocumentVersion [nur Berechtigung]	Gewährt die Berechtigung zum Herunterladen einer bestimmten Dokumentversion	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetCurrentUser	Gewährt die Berechtigung zum Abrufen der Details des aktuellen Benutzers	Lesen			
GetDocument	Gewährt die Berechtigung zum Abrufen des angegebenen Dokumentobjekts	Lesen			
GetDocumentPath	Gewährt die Berechtigung zum Abrufen der Pfadinformationen (die Hierarchie aus dem Stammordner) für das angeforderte Dokument	Lesen			
GetDocumentVersion	Gewährt die Berechtigung zum Abrufen von Versionsmetadaten für das angegebene Dokument	Lesen			
GetFolder	Gewährt die Berechtigung zum Abrufen der Metadaten des angegebenen Ordners	Lesen			
GetFolderPath	Gewährt die Berechtigung zum Abrufen der Pfadinformationen (die Hierarchie aus dem Stammordner) für den angegebenen Ordner	Lesen			
GetGroup [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen von Details für die angegebene Gruppe	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetResources	Gewährt die Berechtigung zum Abrufen einer Sammlung von Ressourcen	Lesen			
InitiateDocumentVersionUpload	Gewährt die Berechtigung zum Erstellen eines neuen Dokument- und Versionsobjekts	Schreiben			
RegisterDirectory [nur Berechtigung]	Gewährt die Berechtigung zum Registrieren eines Verzeichnisses	Schreiben			
RemoveAllResourcePermissions	Gewährt die Berechtigung zum Entfernen aller Berechtigungen von der angegebenen Ressource	Schreiben			
RemoveResourcePermission	Gewährt die Berechtigung zum Entfernen der Berechtigung für den angegebenen Prinzipal aus der angegebenen Ressource	Schreiben			
RestoreDocumentVersions	Gewährt die Berechtigung zum Wiederherstellen der Versionen eines angegebenen Dokuments	Schreiben			
SearchResources	Gewährt die Berechtigung zum Durchsuchen von Metadaten und dem Inhalt von Ressourcen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
StartInstanceExport [nur Berechtigung]	Erteilt die Berechtigung, einen Export für eine Instanz zu starten	Schreiben	organization*		
UpdateDocument	Gewährt die Berechtigung zum Aktualisieren der angegebenen Attribute des angegebenen Dokuments	Schreiben			
UpdateDocumentVersion	Gewährt die Berechtigung zum Ändern des Status der Dokumentversion in AKTIV	Schreiben			
UpdateFolder	Gewährt die Berechtigung zum Aktualisieren der angegebenen Attribute des angegebenen Ordners	Schreiben			
UpdateInstanceAlias [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren eines Instance-Alias	Schreiben			
UpdateUser	Erteilt die Erlaubnis, die angegebenen Attribute des angegebenen Benutzers zu aktualisieren, und gewährt oder widerruft Administratorrechte für die Amazon-Website WorkDocs	Schreiben			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateUserAdministrativeSettings [nur Berechtigung]	Erteilt die Berechtigung zum Aktualisieren der administrativen Einstellungen für einen Benutzer	Schreiben			

Von Amazon definierte Ressourcentypen WorkDocs

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
organization	`arn:${Partition}:workdocs:${Region}:${Account}:organization/${ResourceId}`	

Zustandsschlüssel für Amazon WorkDocs

WorkDocs hat keine dienstspezifischen Kontextschlüssel, die `Condition` in Richtlinienerklärungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon WorkLink

Amazon WorkLink (Servicepräfix: `worklink`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon WorkLink definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen

unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateDomain	Gewährt die Berechtigung zum Verknüpfen einer Domain mit einer Amazon WorkLink-Flotte	Write	fleet*		
AssociateWebsiteAuthorizationProvider	Gewährt die Berechtigung zum Verknüpfen eines Website-Autorisierungsanbieters mit einer Amazon WorkLink-Flotte	Write	fleet*		
AssociateWebsiteCe	Gewährt die Berechtigung zum Verknüpfen einer Website-Zertifizierungsstelle	Write	fleet*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
rtificate Authority	mit einer Amazon WorkLink-Flotte				
CreateFleet	Gewährt die Berechtigung zum Erstellen einer Amazon WorkLink-Flotte	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFleet	Gewährt die Berechtigung zum Löschen einer Amazon WorkLink-Flotte	Write	fleet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeAuditStreamConfiguration	Gewährt die Berechtigung zum Beschreiben der Konfiguration des Audit-Streams für eine Amazon WorkLink-Flotte	Read	fleet*		
DescribeCompanyNetworkConfiguration	Gewährt die Berechtigung zum Beschreiben der Unternehmensnetzwerkkonfiguration für eine Amazon WorkLink-Flotte	Read	fleet*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeDevice	Gewährt die Berechtigung zum Beschreiben von Details eines Geräts, das einer Amazon WorkLink-Flotte zugeordnet ist	Read	fleet*		
DescribeDevicePolicyConfiguration	Gewährt die Berechtigung zum Beschreiben der Geräterichtlinienkonfiguration für eine Amazon WorkLink-Flotte	Read	fleet*		
DescribeDomain	Gewährt die Berechtigung zum Beschreiben von Details zu einer Domain, die einer Amazon WorkLink-Flotte zugeordnet ist	Read	fleet*		
DescribeFleetMetadata	Gewährt die Berechtigung zum Beschreiben von Metadaten einer Amazon WorkLink-Flotte	Read	fleet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeIdentityProviderConfiguration	Gewährt die Berechtigung zum Beschreiben der Identitätsanbieterkonfiguration für eine Amazon WorkLink-Flotte	Read	fleet*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeWebsiteCertificateAuthority	Gewährt die Berechtigung zum Beschreiben einer Website-Zertifizierungsstelle, die einer Amazon WorkLink-Flotte zugeordnet ist	Read	fleet*		
DisassociateDomain	Gewährt die Berechtigung zum Aufheben der Mapping einer Domain zu einer Amazon WorkLink-Flotte	Write	fleet*		
DisassociateWebsiteAuthorizationProvider	Gewährt die Berechtigung zum Aufheben der Mapping eines Website-Autorisierungsanbieters zu einer Amazon WorkLink-Flotte	Write	fleet*		
DisassociateWebsiteCertificateAuthority	Gewährt die Berechtigung zum Aufheben der Mapping einer Website-Zertifizierungsstelle zu einer Amazon WorkLink-Flotte	Write	fleet*		
ListDevices	Gewährt die Berechtigung zum Auflisten der Geräte, die einer Amazon WorkLink-Flotte zugeordnet sind	List	fleet*		
ListDomains	Gewährt die Berechtigung zum Auflisten der zugehörigen Domains für eine Amazon WorkLink-Flotte	List	fleet*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListFleets	Gewährt die Berechtigung zum Auflisten der Amazon WorkLink-Flotten, die dem Konto zugeordnet sind	List			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Read	fleet*		
ListWebsiteAuthorizationProviders	Gewährt die Berechtigung zum Auflisten der Website-Autorisierungsanbieter für eine Amazon WorkLink-Flotte	List	fleet*		
ListWebsiteCertificateAuthorities	Gewährt die Berechtigung zum Auflisten der Website-Zertifizierungsstellen, die einer Amazon WorkLink-Flotte zugeordnet sind	List	fleet*		
RestoreDomainAccess	Gewährt die Berechtigung zum Wiederherstellen des Zugriffs auf eine Domain, die einer Amazon WorkLink-Flotte zugeordnet ist	Write	fleet*		
RevokeDomainAccess	Gewährt die Berechtigung zum Widerrufen des Zugriffs auf eine Domain, die einer Amazon WorkLink-Flotte zugeordnet ist	Write	fleet*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SearchEntity [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Geräten für eine Amazon WorkLink-Flotte	List	fleet*		
SignOutUser	Gewährt die Berechtigung zum Abmelden eines Benutzers aus einer Amazon WorkLink-Flotte	Write	fleet*		
TagResource	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Tags zu einer Ressource	Markieren	fleet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Gewährt die Berechtigung, ein oder mehrere Tags aus einer Ressource zu entfernen	Markieren	fleet*		
				aws:TagKeys	
UpdateAuditStreamConfiguration	Gewährt die Berechtigung zum Aktualisieren der Konfiguration des Audit-Streams für eine Amazon WorkLink-Flotte	Write	fleet*		
UpdateCompanyNetworkConfiguration	Gewährt die Berechtigung zum Aktualisieren der Unternehmensnetzwerkkonfiguration für eine Amazon WorkLink-Flotte	Write	fleet*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateDevicePolicyConfiguration	Gewährt die Berechtigung zum Aktualisieren der Geräterichtlinienkonfiguration für eine Amazon WorkLink-Flotte	Write	fleet*		
UpdateDomainMetadata	Gewährt die Berechtigung zum Aktualisieren der Metadaten für eine Domain, die einer Amazon WorkLink-Flotte zugeordnet ist	Write	fleet*		
UpdateFleetMetadata	Gewährt die Berechtigung zum Aktualisieren der Metadaten einer Amazon WorkLink-Flotte	Write	fleet*		
UpdateIdentityProviderConfiguration	Gewährt die Berechtigung zum Aktualisieren der Identitätsanbieterkonfiguration für eine Amazon WorkLink-Flotte	Write	fleet*		

Von Amazon WorkLink definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
fleet	`arn:${Partition}:worklink::${Account}:fleet/${FleetName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon WorkLink

Amazon WorkLink definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüssel-Wert-Paaren in der Anforderung.	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert Aktionen basierend auf den Tag-Schlüssel-Wert-Paaren, die an die Ressource angefügt wurden.	Zeichenfolge
aws:TagKeys	Filtert Aktionen basierend auf dem Vorhandensein von Tag-Schlüsseln in der Anforderung.	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon WorkMail

Amazon WorkMail (Service-Präfix:`workmail`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.

- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon definierte Aktionen WorkMail
- Von Amazon definierte Ressourcentypen WorkMail
- Zustandsschlüssel für Amazon WorkMail

Von Amazon definierte Aktionen WorkMail

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AllowVendedLogDeliveryForResource [nur Berechtigung]	Erteilt die Erlaubnis, die Übermittlung von versendeten Protokollen für WorkMail Audit-Logs zu konfigurieren	Schreiben	organization*		
AssociateDelegateToResource	Gewährt die Berechtigung zum Hinzufügen eines Mitglieds (Benutzer oder Gruppe) zur Gruppe von Stellvertretern der Ressource	Write	organization*		
AssociateMemberToGroup	Gewährt die Berechtigung zum Hinzufügen eines Mitglieds (Benutzer oder Gruppe) zum Satz der Gruppe	Schreiben	organization*		
AssumeImpersonationRole	Erteilt die Erlaubnis, eine Identitätswechselrolle für die angegebene Amazon-Or	Schreiben	organization*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
	ganisation zu übernehmen WorkMail				
CancelMailboxExportJob	Gewährt die Berechtigung zum Abbrechen eines aktuell ausgeführten Postfachexportauftrags	Schreiben	organization*		
CreateAlias	Erteilt die Erlaubnis, der Gruppe eines bestimmten Mitglieds (Benutzers oder Gruppe) von einen Alias hinzuzufügen WorkMail	Schreiben	organization*		
CreateAvailabilityConfiguration	Erteilt die Erlaubnis, eine AvailabilityConfiguration für die angegebene WorkMail Amazon-Organisation und -Domain zu erstellen	Schreiben	organization*		
CreateGroup	Erteilt die Erlaubnis, eine Gruppe zu erstellen, die verwendet werden kann, WorkMail indem der RegisterToWorkMail Vorgang aufgerufen wird	Schreiben	organization*		
CreateImpersonationRole	Erteilt die Erlaubnis, eine Identitätswechselrolle für die angegebene Amazon-Organisation zu erstellen WorkMail	Schreiben	organization*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateInboundMailFlowRule [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer E-Mail-Flussregel für eingehenden Datenverkehr, die für alle an eine Organisation gesendeten E-Mails gilt	Write	organization*		
CreateMailDomain [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer Mail-Domain	Schreiben	organization*		
CreateMobileDeviceAccessRule	Gewährt die Berechtigung zum Erstellen einer neuen Zugriffsregel für Mobilgeräte	Schreiben	organization*		
CreateOrganization	Erteilt die Erlaubnis, eine neue WorkMail Amazon-Organisation zu gründen	Schreiben			
CreateOutboundMailFlowRule [nur Berechtigung]	Gewährt die Berechtigung zum Erstellen einer E-Mail-Flussregel für ausgehenden Datenverkehr, die für alle von einer Organisation gesendeten E-Mails gilt	Schreiben	organization*		
CreateResource	Erteilt die Erlaubnis, eine neue WorkMail Ressource zu erstellen	Schreiben	organization*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateSmtpGateway [nur Berechtigung]	Erteilt einer Organisation die Erlaubnis, ein SMTP-Gateway zu registrieren WorkMail	Schreiben	organization*		
CreateUser	Erteilt die Berechtigung zum Erstellen eines Benutzers, der anschließend durch Aufrufen des RegisterToWorkMail Vorgangs aktiviert werden kann	Schreiben	organization*		
DeleteAccessControlRule	Gewährt die Berechtigung zum Löschen einer Zugriffssteuerungsregel	Write	organization*		
DeleteAlias	Gewährt die Berechtigung zum Entfernen einer oder mehrerer angegebenen Aliasse aus einer Reihe von Aliassen für einen bestimmten Benutzer	Schreiben	organization*		
DeleteAvailabilityConfiguration	Erteilt die Erlaubnis, die AvailabilityConfiguration für die angegebene WorkMail Amazon-Organisation und Domain zu löschen	Schreiben	organization*		
DeleteEmailMonitoringConfiguration	Gewährt die Berechtigung zum Löschen der E-Mail-Überwachungskonfiguration für eine Organisation	Schreiben	organization*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteGroup	Erteilt die Erlaubnis zum Löschen einer Gruppe von WorkMail	Schreiben	organization*		
DeleteImpersonationRole	Erteilt die Erlaubnis, eine Identitätswechselrolle für die angegebene Amazon-Organisation zu löschen WorkMail	Schreiben	organization*		
DeleteInboundMailFlowRule [nur Berechtigung]	Gewährt die Berechtigung zum Entfernen einer E-Mail-Flussregel für eingehenden Verkehr, damit sie nicht mehr auf E-Mails angewendet wird, die von einer Organisation gesendet werden	Write	organization*		
DeleteMailDomain [nur Berechtigung]	Gewährt die Berechtigung zum Entfernen einer nicht verwendeten Mail-Domain aus einer Organisation	Write	organization*		
DeleteMailboxPermissions	Gewährt die Berechtigung zum Löschen von Berechtigungen, die einem Mitglied (Benutzer oder Gruppe) gewährt wurden	Write	organization*		
DeleteMobileDevice [nur Berechtigung]	Gewährt die Berechtigung zum Entfernen eines Mobilgeräts von einem Benutzer	Schreiben	organization*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteMobileDeviceAccessOverride	Gewährt die Berechtigung zum Löschen einer Zugriffs-Überschreibung für Mobilgeräte	Schreiben	organization*		
DeleteMobileDeviceAccessRule	Gewährt die Berechtigung zum Löschen einer Zugriffsregel für Mobilgeräte	Schreiben	organization*		
DeleteOrganization	Erteilt die Erlaubnis, eine WorkMail Amazon-Organisation und alle zugrunde liegenden AWS Ressourcen zu löschen, die von Amazon WorkMail als Teil der Organisation verwaltet werden	Schreiben	organization*		
DeleteOutboundMailFlowRule [nur Berechtigung]	Gewährt die Berechtigung zum Entfernen einer E-Mail-Flussregel für ausgehenden Verkehr, sodass sie nicht mehr auf E-Mails angewendet wird, die von einer Organisation gesendet werden	Write	organization*		
DeleteResource	Gewährt die Berechtigung zum Löschen der angegebenen Ressource	Write	organization*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteRetentionPolicy	Gewährt die Berechtigung zum Löschen der Aufbewahrungsrichtlinie basierend auf den bereitgestellten Organisations- und Richtlinienbezeichnern	Write	organization*		
DeleteSmtpGateway [nur Berechtigung]	Gewährt die Berechtigung zum Entfernen eines SMTP-Gateways aus einer Organisation	Schreiben	organization*		
DeleteUser	Erteilt die Erlaubnis, einen Benutzer aus WorkMail und allen nachfolgenden Systemen zu löschen	Schreiben	organization*		
DeregisterFromWorkMail	Erteilt die Berechtigung, einen Benutzer, eine Gruppe oder eine Ressource als nicht mehr verwendet zu markieren WorkMail	Schreiben	organization*		
DeregisterMailDomain	Gewährt die Berechtigung zum Entfernen einer Mail-Domain aus einer Organisation	Schreiben	organization*		
DescribeEmailMonitoringConfiguration	Gewährt die Berechtigung zum Abrufen der E-Mail-Überwachungskonfiguration für eine Organisation	Lesen	organization*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeEntity	Gewährt die Berechtigung zum Lesen der Details einer Entität	Lesen	organization*		
DescribeGroup	Gewährt die Erlaubnis zum Lesen der Details für eine Gruppe	Auflisten	organization*		
DescribeInboundDmarcSettings	Gewährt die Berechtigung zum Lesen der Einstellungen in einer DMARC-Richtlinie für eine bestimmte Organisation	Lesen	organization*		
DescribeInboundMailFlowRule [nur Berechtigung]	Gewährt die Berechtigung zum Lesen der Details einer für eine Organisation konfigurierten E-Mail-Flussregel für eingehenden Datenverkehr	Read	organization*		
DescribeMailDomains [nur Berechtigung]	Gewährt die Berechtigung zum Anzeigen der Details aller E-Mail-Domains, die der Organisation zugeordnet sind	Auflisten	organization*		
DescribeMailboxExportJob	Gewährt die Berechtigung zum Abrufen von Details einer Postfachexportaufgabe	Read	organization*		
DescribeOrganization	Gewährt die Erlaubnis zum Lesen der Details einer Organisation	List	organization*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeOutboundMailFlowRule [nur Berechtigung]	Gewährt die Berechtigung zum Lesen der Details einer für eine Organisation konfigurierten E-Mail-Flussregel für ausgehenden Datenverkehr	Read	organization*		
DescribeResource	Gewährt die Berechtigung zum Lesen der Details für eine Ressource	List	organization*		
DescribeSmtpGateway [nur Berechtigung]	Gewährt die Berechtigung zum Lesen der Details eines bei einer Organisation registrierten SMTP-Gateways	Read	organization*		
DescribeUser	Gewährt die Berechtigung zum Lesen von Details für einen Benutzer	Auflisten	organization*		
DisassociateDelegateFromResource	Gewährt die Berechtigung, ein Mitglied aus der Gruppe der Stellvertreter der Ressource zu entfernen	Write	organization*		
DisassociateMemberFromGroup	Gewährt die Berechtigung, ein Mitglied aus einer Gruppe zu entfernen	Write	organization*		
EnableMailDomain [nur Berechtigung]	Gewährt die Berechtigung zum Aktivieren einer Mail-Domain in der Organisation	Schreiben	organization*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAccessControlEffect	Gewährt die Berechtigung zum Abrufen der Auswirkungen der Zugriffssteuerungsregeln, wenn sie auf eine angegebene IPv4-Adresse, Zugriffsprotokollaktion oder Benutzer-ID angewendet werden	Read	organization*		
GetDefaultRetentionPolicy	Gewährt die Berechtigung zum Abrufen der auf Organisationsebene verbundenen Aufbewahrungsrichtlinie	Lesen	organization*		
GetImpersonationRole	Erteilt die Erlaubnis, eine Identitätswechselrolle für die angegebene Amazon-Organisation abzurufen WorkMail	Lesen	organization*		
GetImpersonationRoleEffect	Gewährt die Berechtigung, die Wirkung der Regeln abzurufen, die einer Identitätswechselrolle für einen bestimmten Benutzer zugeordnet sind	Lesen	organization*		
GetJournalingRules [nur Berechtigung]	Gewährt die Berechtigung zum Lesen der konfigurierten Journal- und Fallback-E-Mail-Adressen für das E-Mail-Journal	Lesen	organization*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetMailDomain	Gewährt die Berechtigung zum Abrufen von Details einer bestimmten Mail-Domain in einer Organisation	Lesen	organization*		
GetMailDomainDetails [nur Berechtigung]	Gewährt die Erlaubnis zum Abrufen der Details der E-Mail-Domain	Lesen	organization*		
GetMailboxDetails	Gewährt die Erlaubnis zum Lesen der Details des Postfachs des Benutzers	Read	organization*		
GetMobileDeviceAccessEffect	Gewährt die Berechtigung zum Simulieren der Auswirkungen der Zugriffsregeln für Mobilgeräte für die angegebenen Attribute eines Beispielzugriffsereignisses	Lesen	organization*		
GetMobileDeviceAccessOverride	Gewährt die Berechtigung zum Abrufen einer Zugriffs-Überschreibung für Mobilgeräte	Lesen	organization*		
GetMobileDeviceDetails [nur Berechtigung]	Gewährt die Erlaubnis zum Abrufen der Details des Mobilgeräts	Read	organization*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetMobileDevicesForUser [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen einer Liste der mobilen Geräte, die dem Benutzer zugeordnet sind	Read	organization*		
GetMobilePolicyDetails [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen der Details der Richtlinie für Mobilgeräte, die der Organisation zugeordnet ist	Read	organization*		
ListAccessControlRules	Gewährt die Berechtigung zum Auflisten der Zugriffssteuerungsregeln	Lesen	organization*		
ListAliases	Gewährt die Berechtigung zum Auflisten der Aliasse, die mit einer bestimmten Entität verknüpft sind	Auflisten	organization*		
ListAvailabilityConfigurations	Erteilt die Erlaubnis, alle Einträge für AvailabilityConfiguration die angegebene WorkMail Amazon-Organisation aufzulisten	Lesen	organization*		
ListGroupMembers	Gewährt die Erlaubnis zum Lesen eines Überblicks über die Mitglieder einer Gruppe. Benutzer und Gruppen können Mitglieder einer Gruppe sein.	List	organization*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListGroups	Gewährt die Erlaubnis zum Auflisten der Zusammenfassungen der Gruppen der Organisation	Auflisten	organization*		
ListGroupsForEntity	Gewährt die Berechtigung zum Auflisten der Gruppen, zu denen eine Entität angehört	Auflisten	organization*		
ListImpersonationRoles	Erteilt die Erlaubnis, die Identitätswechselrollen für die angegebene Amazon-Organisation aufzulisten WorkMail	Auflisten	organization*		
ListInboundMailFlowRules [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der E-Mail-Flussregeln für eingehenden Datenverkehr, die für eine Organisation konfiguriert sind	Auflisten	organization*		
ListMailDomains	Gewährt die Berechtigung zum Auflisten der Mail-Domain für eine bestimmte Organisation	Auflisten	organization*		
ListMailboxExportJobs	Gewährt die Berechtigung zum Auflisten von Postfachexportaufgaben	List	organization*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListMailboxPermissions	Gewährt die Berechtigung zum Auslisten der Postfachberechtigungen, die einem Benutzer, einer Gruppe oder einem Ressourcenpostfach zugeordnet sind	Auflisten	organization*		
ListMobileDeviceAccessOverrides	Gewährt die Berechtigung zum Auflisten der Zugriffs-Überschreibungen für Mobilgeräte	Lesen	organization*		
ListMobileDeviceAccessRules	Gewährt die Berechtigung zum Auflisten der Zugriffsregeln für Mobilgeräte	Lesen	organization*		
ListOrganizations	Gewährt die Berechtigung zum Auflisten der nicht gelöschten Organisationen	List			
ListOutboundMailFlowRules [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten der E-Mail-Flussregeln für ausgehenden Datenverkehr, die für eine Organisation konfiguriert sind	List	organization*		
ListResourceDelegates	Gewährt die Berechtigung zum Auflisten von Stellvertretern, die einer Ressource zugeordnet sind	List	organization*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListResources	Gewährt die Berechtigung zum Auflisten der Ressourcen der Organisation.	List	organization*		
ListSmtpGateways [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von SMTP-Gateways, die bei der Organisation registriert sind	Auflisten	organization*		
ListTagsForResource	Erteilt die Erlaubnis, die auf eine WorkMail Amazon-Organisationsressource angewendeten Tags aufzulisten	Auflisten	organization*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ListUsers	Gewährt die Berechtigung zum Auflisten der Benutzer der Organisation.	List	organization*		
PutAccessControlRule	Gewährt die Berechtigung zum Hinzufügen einer neuen Zugriffssteuerungsregel	Schreiben	organization*		
PutEmailMonitoringConfiguration	Gewährt die Berechtigung zum Hinzufügen der E-Mail-Überwachungskonfiguration für eine Organisation	Schreiben	organization*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutInboundDmarcSettings	Gewährt die Berechtigung zum Aktivieren oder Deaktivieren einer DMARC-Richtlinie für eine bestimmte Organisation	Schreiben	organization*		
PutMailboxPermissions	Gewährt die Berechtigung zum Festlegen von Berechtigungen für einen Benutzer, eine Gruppe oder eine Ressource und ersetzt alle vorhandenen Berechtigungen	Schreiben	organization*		
PutMobileDeviceAccessOverride	Gewährt die Berechtigung zum Hinzufügen oder Aktualisieren einer Zugriffs-Überschreibung für Mobilgeräte	Schreiben	organization*		
PutRetentionPolicy	Gewährt die Berechtigung zum Hinzufügen oder Aktualisieren der Aufbewahrungsrichtlinie	Schreiben	organization*		
RegisterMailDomain	Gewährt die Berechtigung zum Registrieren einer neuen Mail-Domain in einer Organisation	Schreiben	organization*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
RegisterToWorkMail	Gewährt die Berechtigung zum Registrieren vorhandener und deaktivierter Benutzer, Gruppen oder Ressourcen zur Verwendung, indem ein Postfach und Kalenderfunktionen zugeordnet werden	Schreiben	organization*		
ResetPassword	Gewährt die Berechtigung, dem Administrator das Zurücksetzen des Kennworts für einen Benutzer zu erlauben	Write	organization*		
SearchMembers [nur Berechtigung]	Gewährt die Berechtigung zum Durchführen einer Präfixsuche, um einen bestimmten Benutzer in einer E-Mail-Gruppe zu finden	Read	organization*		
SetDefaultMailDomain [nur Berechtigung]	Gewährt die Berechtigung zum Festlegen der Standard-Mail-Domain für die Organisation	Write	organization*		
SetJournalingRules [nur Berechtigung]	Gewährt die Berechtigung zum Festlegen von Journal- und Fallback-E-Mail-Adressen für das E-Mail-Journal	Write	organization*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
SetMobilePolicyDetails [nur Berechtigung]	Gewährt die Berechtigung zum Festlegen der Details einer mobilen Richtlinie, die der Organisation zugeordnet ist	Write	organization*		
StartMailboxExportJob	Gewährt die Berechtigung zum Starten eines neuen Postfachexportauftrags	Schreiben	organization*		
TagResource	Erteilt die Erlaubnis, die angegebene WorkMail Amazon-Organisationsressource zu taggen	Tagging	organization*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestAvailabilityConfiguration	Erteilt die Berechtigung, einen Test an einem Verfügbarkeitsanbieter durchzuführen, um sicherzustellen, dass der Zugriff erlaubt ist	Lesen	organization*		
TestInboundMailFlowRules [nur Berechtigung]	Gewährt die Berechtigung zum Testen, welche Regeln für eingehenden Datenverkehr für eine E-Mail mit einem bestimmten Sender und Empfänger gelten	Write	organization*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
TestOutboundMailFlowRules [nur Berechtigung]	Gewährt die Berechtigung zum Testen, welche Regeln für ausgehenden Datenverkehr für eine E-Mail mit einem bestimmten Sender und Empfänger gelten	Schreiben	organization*		
UntagResource	Erteilt die Erlaubnis, die angegebene WorkMail Amazon-Organisationsressource zu entkennzeichnen	Tagging	organization*		
				aws:TagKeys	
UpdateAvailabilityConfiguration	Erteilt die Erlaubnis, ein vorhandenes AvailabilityConfiguration für die angegebene WorkMail Amazon-Organisation und -Domain zu aktualisieren	Schreiben	organization*		
UpdateDefaultMailDomain	Gewährt die Berechtigung zum Aktualisieren, welche Domain die Standard-Domain für eine Organisation ist	Schreiben	organization*		
UpdateGroup	Gewährt die Berechtigung zum Aktualisieren der Details einer Gruppe	Schreiben	organization*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateImpersonationRole	Erteilt die Erlaubnis, eine bestehende Identitätswechselrolle für die angegebene Amazon-Organisation zu aktualisieren WorkMail	Schreiben	organization*		
UpdateInboundMailFlowRule [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren der Details einer E-Mail-Flussregel für eingehenden Datenverkehr, die für alle an eine Organisation gesendeten E-Mails gilt	Write	organization*		
UpdateMailboxQuota	Gewährt die Berechtigung zum Aktualisieren der maximalen Größe (in MB) des Postfachs des Benutzers	Schreiben	organization*		
UpdateMobileDeviceAccessRule	Gewährt die Berechtigung zum Aktualisieren einer Zugriffsregel für Mobilgeräte	Schreiben	organization*		
UpdateOutboundMailFlowRule [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren der Details einer E-Mail-Flussregel für ausgehenden Datenverkehr, die für alle von einer Organisation gesendeten E-Mails gilt	Write	organization*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdatePrimaryEmailAddress	Gewährt die Berechtigung zum Aktualisieren der primären E-Mail für einen Benutzer, eine Gruppe oder eine Ressource	Write	organization*		
UpdateResource	Gewährt die Berechtigung zum Aktualisieren von Details für die angegebene Ressource	Write	organization*		
UpdateSmtpGateway [nur Berechtigung]	Gewährt die Berechtigung zum Aktualisieren der Details eines vorhandenen SMTP-Gateways, das bei einer Organisation registriert ist	Schreiben	organization*		
UpdateUser	Gewährt die Berechtigung zum Aktualisieren der Details eines Benutzers	Schreiben	organization*		
WipeMobileDevice [nur Berechtigung]	Gewährt die Berechtigung zum Remote-Zurücksetzen des Mobilgeräts, das dem Konto eines Benutzers zugeordnet ist	Schreiben	organization*		

Von Amazon definierte Ressourcentypen WorkMail

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie

einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
organization	`arn:${Partition}:workmail:${Region}:${Account}:organization/${ResourceId}`	aws:ResourceTag/${TagKey}

Zustandsschlüssel für Amazon WorkMail

Amazon WorkMail definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff nach den Tag-Schlüssel-Wert-Paaren, die in der Anforderung weitergegeben werden	String
aws:ResourceTag/${TagKey}	Filtert Aktionen nach Tag-Schlüsselwertpaaren, die der Ressource angefügt sind	String
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon WorkMail Message Flow

Amazon WorkMail Message Flow (Servicepräfix: `workmailmessageflow`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon WorkMail Message Flow definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen

Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetRawMessageContent	Gewährt die Berechtigung zum Lesen des Inhalts von E-Mail-Nachrichten mit der angegebenen Mitteilungs-ID.	Lesen	RawMessage*		
PutRawMessageContent	Gewährt die Berechtigung zum Lesen des Inhalts von E-Mail-Nachrichten mit der angegebenen Mitteilungs-ID.	Schreiben	RawMessage*		

Von Amazon WorkMail Message Flow definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
RawMessage	`arn:${Partition}:workmailmessageflow:${Region}:${Account}:message/${OrganizationId}/${Context}/${MessageId}`	

Bedingungsschlüssel für Amazon WorkMail Message Flow

WorkMail Message Flow besitzt keine servicespezifischen Kontextschlüssel, die im `Condition`-Element von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon WorkSpaces

Amazon WorkSpaces (Service-Präfix:`workspaces`) stellt die folgenden dienstspezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Vorgänge an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon definierte Aktionen WorkSpaces
- Von Amazon definierte Ressourcentypen WorkSpaces
- Zustandsschlüssel für Amazon WorkSpaces

Von Amazon definierte Aktionen WorkSpaces

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AcceptAccountLinkInvitation	Erteilt die Erlaubnis, Einladungen von anderen AWS Konten anzunehmen, die dieselbe Konfiguration für WorkSpaces BYOL verwenden	Schreiben			
AssociateConnectionAlias	Gewährt die Berechtigung zum Verknüpfen von Verbindungsaliasen mit Verzeichnissen	Write	connectionalias*		
			directoryid*		
AssociateIpGroups	Gewährt die Berechtigung zum Verknüpfen von IP-Zugriffskontrollgruppen mit Verzeichnissen	Schreiben	directoryid*		
			workspaceipgroup*		
AssociateWorkspaceApplication	Erteilt die Berechtigung, eine Workspace-Anwendung einem zuzuordnen WorkSpace	Schreiben	workspaceapplication*		
			workspaceid*		
				aws:ResourceTag/${TagKey}	
AuthorizeIpRules	Gewährt die Berechtigung zum Hinzufügen von Regeln zu IP-Zugriffskontrollgruppen	Schreiben	workspaceipgroup*		workspaces:UpdateR

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					ulesOfIpGroup
CopyWorkspaceImage	Erteilt die Erlaubnis, ein WorkSpace Bild zu kopieren	Schreiben	workspaceimage*		workspaces:DescribeWorkspaceImages
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAccountLinkInvitation	Erteilt die Erlaubnis, andere AWS Konten einzuladen, dieselbe Konfiguration für WorkSpaces BYOL zu verwenden	Schreiben			
CreateConnectClientAddIn	Gewährt die Berechtigung zum Erstellen eines Amazon-Connect-Client-Add-Ins in einem Verzeichnis	Schreiben	directoryid*		
CreateConnectionAlias	Gewährt die Berechtigung zum Erstellen von Verbindungsaliasen zur Verwendung mit regionsübergreifender Umleitung	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateIpGroup	Gewährt die Berechtigung zum Erstellen von IP-Zugriffskontrollgruppen	Schreiben		aws:RequestTag/${TagKey} aws:TagKeys	
CreateStandbyWorkspaces	Erteilt die Erlaubnis, einen oder mehrere Standby-Server zu erstellen WorkSpaces	Schreiben	directoryid*		
			workspaceid*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTags	Erteilt die Erlaubnis, Tags für WorkSpaces Ressourcen zu erstellen	Tagging		aws:RequestTag/${TagKey} aws:TagKeys	
CreateUpdatedWorkspaceImage	Erteilt die Erlaubnis, ein aktualisiertes WorkSpace Bild zu erstellen	Schreiben	workspaceimage*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspaceBundle	Erteilt die Erlaubnis, ein WorkSpace Bundle zu erstellen	Schreiben	workspacebundle*		workspaces:CreateTags
			workspaceimage*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspaceImage	Erteilt die Erlaubnis, ein neues WorkSpace Image zu erstellen	Schreiben	workspaceid*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspaces	Erteilt die Erlaubnis, eines oder mehrere zu erstellen WorkSpaces	Schreiben	directoryid*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			workspacebundle*		
			workspaceid*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccountLinkInvitation	Erteilt die Erlaubnis, Einladungen an andere AWS Konten zu löschen, die dieselbe Konfiguration für WorkSpaces BYOL verwenden	Schreiben			
DeleteClientBranding	Erteilt die Berechtigung zum Löschen von AWS WorkSpaces Client-Branding-Daten in einem Verzeichnis	Schreiben	directoryid*		
DeleteConnectClientAddIn	Gewährt die Berechtigung zum Löschen eines Amazon-Connect-Client-Add-Ins, das in einem Verzeichnis konfiguriert ist	Schreiben	directoryid*		
DeleteConnectionAlias	Gewährt die Berechtigung zum Löschen eines Verbindungs-Aliases	Write	connectionalias*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteIpGroup	Gewährt Berechtigung zum Löschen von IP-Zugriffskontrolgruppen	Schreiben	workspaceipgroup*		
DeleteTags	Erteilt die Berechtigung zum Löschen von Tags aus WorkSpaces Ressourcen	Tagging		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteWorkspaceBundle	Erteilt die Erlaubnis zum Löschen von WorkSpace Bundles	Schreiben	workspacebundle*		
DeleteWorkspaceImage	Erteilt die Erlaubnis zum Löschen von Bildern WorkSpace	Schreiben	workspaceimage*		
DeployWorkspaceApplications	Erteilt die Berechtigung zur Bereitstellung aller ausstehenden Workspace-Anwendungen auf einem WorkSpace	Schreiben	workspaceid*		
				aws:ResourceTag/${TagKey}	
DeregisterWorkspaceDirectory	Erteilt die Erlaubnis, Verzeichnisse für die Verwendung mit Amazon zu deregistrieren WorkSpaces	Schreiben	directoryid*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeAccount	Erteilt die Erlaubnis, die Konfiguration von Bring Your Own License (BYOL) für Konten abzurufen WorkSpaces	Lesen			
DescribeAccountModifications	Erteilt die Erlaubnis, Änderungen an der Konfiguration von Bring Your Own License (BYOL) für Konten abzurufen WorkSpaces	Lesen			
DescribeApplicationAssociations	Erteilt die Berechtigung zum Abrufen von Informationen über Ressourcen, die einer WorkSpace Anwendung zugeordnet sind	Auflisten	workspaceapplication*		
				aws:ResourceTag/${TagKey}	
DescribeApplications	Erteilt die Erlaubnis, Informationen über WorkSpace Anwendungen zu erhalten	Auflisten			
DescribeBundleAssociations	Erteilt die Berechtigung zum Abrufen von Informationen über Ressourcen, die einem WorkSpace Bundle zugeordnet sind	Auflisten	workspacebundle*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeClientBranding	Erteilt die Berechtigung zum Abrufen von AWS WorkSpaces Client-Branding-Daten in einem Verzeichnis	Lesen	directory id*		
DescribeClientProperties	Erteilt die Berechtigung zum Abrufen von Informationen über WorkSpaces Kunden	Auflisten	directory id*		
DescribeConnectClientAddIns	Gewährt die Berechtigung zum Abrufen einer Liste von Amazon-Connect-Client-Add-Ins, die erstellt wurden	Auflisten	directory id*		
DescribeConnectionAliasPermissions	Erteilt die Berechtigung zum Abrufen der Berechtigungen, die die Besitzer von Verbindungsaliasnamen anderen AWS Konten für Verbindungsaliase erteilt haben	Lesen	connectionalias*		
DescribeConnectionAliases	Gewährt die Berechtigung zum Abrufen einer Liste, die die für die regionsübergreifende Umleitung verwendeten Verbindungsaliase beschreibt	Lesen			
DescribeImageAssociations	Erteilt die Berechtigung zum Abrufen von Informationen über Ressourcen, die mit einem Bild verknüpft sind WorkSpace	Auflisten	workspaceimage*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeIpGroups	Gewährt die Berechtigung zum Abrufen von Informationen über IP-Zugriffskontrollgruppen	Lesen	workspaceipgroup*		
DescribeTags	Erteilt die Erlaubnis, die Tags für WorkSpaces Ressourcen zu beschreiben	Lesen			
DescribeWorkspaceAssociations	Erteilt die Berechtigung zum Abrufen von Informationen über Ressourcen, die mit einem verknüpft sind WorkSpace	Auflisten	workspaceid*		
				aws:ResourceTag/${TagKey}	
DescribeWorkspaceBundles	Erteilt die Erlaubnis, Informationen über WorkSpace Bundles abzurufen	Auflisten			
DescribeWorkspaceDirectories	Erteilt die Berechtigung zum Abrufen von Informationen über Verzeichnisse, die bei registriert sind WorkSpaces	Lesen			
DescribeWorkspaceImagePermissions	Erteilt die Berechtigung zum Abrufen von Informationen über WorkSpace Bildberechtigungen	Lesen	workspaceimage*		
DescribeWorkspaceImages	Erteilt die Erlaubnis zum Abrufen von Informationen über WorkSpace Bilder	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DescribeWorkspaceSnapshots	Erteilt die Berechtigung zum Abrufen von Informationen über WorkSpace Schnappschüsse	Auflisten	workspaceid*		
DescribeWorkspaces	Erteilt die Erlaubnis zum Abrufen von Informationen über WorkSpaces	Auflisten			
DescribeWorkspacesConnectionStatus	Erteilt die Berechtigung zum Abrufen des Verbindungsstatus von WorkSpaces	Lesen			
DisassociateConnectionAlias	Gewährt die Berechtigung zum Trennen von Verbindungsaliasen von Verzeichnissen	Write	connectionalias*		
DisassociateIpGroups	Gewährt die Berechtigung zum Trennen von IP-Zugriffskontrollgruppen von Verzeichnissen	Schreiben	directoryid*		
			workspaceipgroup*		
DisassociateWorkspaceApplication	Erteilt die Berechtigung, die Zuordnung einer Workspace-Anwendung zu einem zu trennen WorkSpace	Schreiben	workspaceapplication*		
			workspaceid*		
				aws:ResourceTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetAccountLink	Erteilt die Berechtigung zum Abrufen eines Links mit einem anderen AWS Konto zur gemeinsamen Nutzung der Konfiguration für BYOL WorkSpaces	Lesen			
ImportClientBranding	Erteilt die Erlaubnis, AWS WorkSpaces Client-Branding-Daten in ein Verzeichnis zu importieren	Schreiben	directoryid*		
ImportWorkspaceImage	Erteilt die Erlaubnis, Bring Your Own License (BYOL) - Bilder in Amazon zu importieren WorkSpaces	Schreiben			ec2:DescribeImages ec2:ModifyImageAttribute
ListAccountLinks	Erteilt die Genehmigung zum Abrufen von Links zu den AWS Konten, die Ihre Konfiguration für WorkSpaces BYOL gemeinsam haben	Auflisten			
ListAvailableManagementCidrRanges	Erteilt die Erlaubnis, die verfügbaren CIDR-Bereiche aufzulisten, um Bring Your Own License (BYOL) für Konten zu aktivieren WorkSpaces	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
MigrateWorkspace	Erteilt die Erlaubnis zur Migration WorkSpaces	Schreiben	workspacebundle*		
			workspaceid*		
ModifyAccount	Erteilt die Erlaubnis, die Konfiguration von Bring Your Own License (BYOL) für WorkSpaces Konten zu ändern	Schreiben			
ModifyCertificateBasedAuthProperties	Gewährt die Berechtigung zum Ändern der zertifikatsbasierten Autorisierungseigenschaften eines Verzeichnisses	Schreiben	directoryid*		
ModifyClientProperties	Erteilt die Erlaubnis, die Eigenschaften von WorkSpaces Clients zu ändern	Schreiben	directoryid*		
ModifySamlProperties	Gewährt die Berechtigung zum Ändern der SAML-Eigenschaften eines Directorys	Schreiben	directoryid*		
ModifySelfservicePermissions	Erteilt die Berechtigung, die WorkSpace Self-Service-Verwaltungsfunktionen für Ihre Benutzer zu ändern	Berechtigungsverwaltung	directoryid*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ModifyWorkspaceAccessProperties	Erteilt die Berechtigung, anzugeben, mit welchen Geräten und Betriebssystemen Benutzer auf ihre WorkSpaces	Schreiben	directory id*		
ModifyWorkspaceCreationProperties	Erteilt die Berechtigung zum Ändern der Standardeigenschaften, die zum Erstellen verwendet wurden WorkSpaces	Schreiben	directory id*		
ModifyWorkspaceProperties	Erteilt die Berechtigung zum Ändern von WorkSpace Eigenschaften, einschließlich des Ausführungsmodus und des AutoStop Zeitraums	Schreiben	workspace id*		
ModifyWorkspaceState	Erteilt die Erlaubnis, den Status von zu ändern WorkSpaces	Schreiben	workspace id*		
RebootWorkspaces	Erteilt die Erlaubnis zum Neustart WorkSpaces	Schreiben	workspace id*		
RebuildWorkspaces	Erteilt die Erlaubnis zum Neuaufbau WorkSpaces	Schreiben	workspace id*		
RegisterWorkspaceDirectory	Erteilt die Erlaubnis, Verzeichnisse zur Verwendung bei Amazon zu registrieren WorkSpaces	Schreiben	directory id*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
RejectAccountLinkInvitation	Erteilt die Erlaubnis, Einladungen von anderen AWS Konten abzulehnen, die dieselbe Konfiguration für WorkSpaces BYOL verwenden	Schreiben			
RestoreWorkspace	Erteilt die Erlaubnis zur Wiederherstellung WorkSpaces	Schreiben	workspaceid*		
RevokeIpRules	Gewährt die Berechtigung zum Entfernen von Regeln aus IP-Zugriffskontrollgruppen	Schreiben	workspaceipgroup*		workspaces:UpdateRulesOfIpGroup
StartWorkspaces	Erteilt die Erlaubnis zum Starten AutoStop WorkSpaces	Schreiben	workspaceid*		
StopWorkspaces	Erteilt die Erlaubnis zum Beenden AutoStop WorkSpaces	Schreiben	workspaceid*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
Stream	Gewährt die Berechtigung, durch die sich verbundene Benutzer mit ihren vorhandenen Anmeldeinformationen anmelden und ihre WorkSpaces streamen können	Schreiben	directoryid*		
				workspaces:userId	
TerminateWorkspaces	Erteilt die Erlaubnis zum Beenden WorkSpaces	Schreiben	workspaceid*		
UpdateConnectClientAddIn	Gewährt die Berechtigung zum Aktualisieren eines Amazon-Connect-Client-Add-Ins. Verwenden Sie diese Aktion, um den Namen und die Endpunkt-URL eines Amazon-Connect-Client-Add-Ins zu aktualisieren.	Schreiben	directoryid*		
UpdateConnectionAliasPermission	Gewährt die Berechtigung zum Teilen oder Aufheben der Freigabe von Verbindungsaliasen mit anderen Konten	Berechtigungsverwaltung	connectionalias*		
UpdateRulesOfIpGroup	Gewährt die Berechtigung zum Austausch von Regeln für IP-Zugriffskontrollgruppen	Schreiben	workspaceipgroup*		workspaces:AuthorizeIpRules workspaces:RevokeIpRules

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateWorkspaceBundle	Erteilt die Erlaubnis, die in WorkSpace WorkSpace Bundles verwendeten Bilder zu aktualisieren	Schreiben	workspacebundle*		
			workspaceimage*		
UpdateWorkspaceImagePermission	Erteilt die Erlaubnis, WorkSpace Bilder mit anderen Konten zu teilen oder deren Freigabe aufzuheben, indem angegeben wird, ob andere Konten berechtigt sind, das Bild zu kopieren	Berechtigungsverwaltung	workspaceimage*		

Von Amazon definierte Ressourcentypen WorkSpaces

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle „Aktionen“ identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
directoryid	`arn:${Partition}:workspaces:${Region}:${Account}:directory/${DirectoryId}`	aws:ResourceTag/${TagKey}

Ressourcentypen	ARN	Bedingungsschlüssel
workspacebundle	arn:${Partition}:workspaces:${Region}:${Account}:workspacebundle/${BundleId}	aws:ResourceTag/${TagKey}
workspaceid	arn:${Partition}:workspaces:${Region}:${Account}:workspace/${WorkspaceId}	aws:ResourceTag/${TagKey}
workspaceimage	arn:${Partition}:workspaces:${Region}:${Account}:workspaceimage/${ImageId}	aws:ResourceTag/${TagKey}
workspaceipgroup	arn:${Partition}:workspaces:${Region}:${Account}:workspaceipgroup/${GroupId}	aws:ResourceTag/${TagKey}
connectionalias	arn:${Partition}:workspaces:${Region}:${Account}:connectionalias/${ConnectionAliasId}	aws:ResourceTag/${TagKey}
workspaceapplication	arn:${Partition}:workspaces:${Region}:${Account}:workspaceapplication/${WorkSpaceApplicationId}	aws:ResourceTag/${TagKey}

Zustandsschlüssel für Amazon WorkSpaces

Amazon WorkSpaces definiert die folgenden Bedingungsschlüssel, die im `Condition` Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüsseln, die in der Anforderung übergeben werden.	ArrayOfString
workspaces:userId	Filtert den Zugriff nach ID des Workspaces-Benutzers	String

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon WorkSpaces Application Manager

Amazon WorkSpaces Application Manager (Servicepräfix: `wam`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungsschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon WorkSpaces Application Manager definierte Aktionen
- Von Amazon WorkSpaces Application Manager definierte Ressourcentypen
- Bedingungsschlüssel für Amazon WorkSpaces Application Manager

Von Amazon WorkSpaces Application Manager definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AuthenticatePackager [nur Berechtigung]	Erlaubt der Amazon WAM-Packen-Instance den Zugriff auf Ihren Anwendung spaketkatalog.	Write			

Von Amazon WorkSpaces Application Manager definierte Ressourcentypen

Amazon WorkSpaces Application Manager unterstützt nicht die Angabe eines Ressourcen-ARN im `Resource`-Element einer IAM-Richtlinienanweisung. Um den Zugriff auf Amazon WorkSpaces Application Manager zu erlauben, geben Sie `"Resource": "*"` in Ihrer Richtlinie an.

Bedingungsschlüssel für Amazon WorkSpaces Application Manager

WAM umfasst keine servicespezifischen Kontextschlüssel, die im Element `Condition` von Richtlinienanweisungen verwendet werden können. Eine Liste der globalen Kontextschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare Schlüssel für Bedingungen.

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client (Servicepräfix: `thinclient`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von Amazon WorkSpaces ThinClient definierte Aktionen
- Von Amazon WorkSpaces Thin Client definierte Ressourcentypen
- Bedingungsschlüssel für Amazon WorkSpaces Thin Client

Von Amazon WorkSpaces ThinClient definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateEnvironment	Gewährt die Berechtigung zum Erstellen von Umgebungen	Schreiben			
DeleteDevice	Gewährt die Berechtigung zum Löschen von Geräten	Schreiben	device*		
DeleteEnvironment	Gewährt die Berechtigung zum Löschen von Umgebungen	Schreiben	environment*		
DeregisterDevice	Gewährt die Berechtigung zum Aufheben der Registrierung von Geräten	Schreiben	device*		
GetDevice	Gewährt die Berechtigung zum Abrufen von Gerätedetails	Lesen	device*		
GetEnvironment	Gewährt die Berechtigung zum Abrufen von Umgebungsdetails	Lesen	environment*		
GetSoftwareSet	Gewährt die Berechtigung zum Abrufen von Details von Softwaresets	Lesen	softwareset*		
ListDeviceSessions [nur Berechtigung]	Gewährt die Berechtigung zum Auflisten von Gerätesitzungen	Auflisten			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListDevices	Gewährt die Berechtigung zum Auflisten von Geräten.	Auflisten			
ListEnvironments	Gewährt die Berechtigung zum Auflisten von Umgebungen	Auflisten			
ListSoftwareSets	Gewährt die Berechtigung, Softwaresätze aufzulisten	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Auflisten			
TagResource	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Tags zu einer Ressource	Markieren	device		
			environment		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung, ein oder mehrere Tags aus einer Ressource zu entfernen	Markierung	device		
			environment		
				aws:TagKeys	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateDevice	Gewährt die Berechtigung zum Aktualisieren des Geräten	Schreiben	device*		
UpdateEnvironment	Gewährt die Berechtigung zum Aktualisieren von Umgebungen	Schreiben	environment*		
UpdateSoftwareSet	Gewährt die Berechtigung zum Aktualisieren von Softwaresätzen	Schreiben	softwareset*		

Von Amazon WorkSpaces Thin Client definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
environment	`arn:${Partition}:thinclient::${Account}:environment/${EnvironmentId}`	aws:ResourceTag/${TagKey}
device	`arn:${Partition}:thinclient::${Account}:device/${DeviceId}`	aws:ResourceTag/${TagKey}
softwareset	`arn:${Partition}:thinclient::${Account}:softwareset/${SoftwareSetId}`	

Bedingungsschlüssel für Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Bedingungsschlüssel.

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für Amazon WorkSpaces Web

Amazon WorkSpaces Web (Servicepräfix: `workspaces-web`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungsschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

Von Amazon WorkSpaces Web definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in

der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
AssociateBrowserSettings	Gewährt die Berechtigung zum Zuordnen von Browsereinstellungen zu Webportalen	Schreiben	browserSettings*		
			portal*		
AssociateIpAccessSettings	Gewährt die Berechtigung zum Zuordnen von IP-Zugriffseinstellungen zu Webportalen	Schreiben	ipAccessSettings*		
			portal*		
AssociateNetworkSettings	Gewährt die Berechtigung zum Zuordnen von Netzwerkeinstellungen zu Webportalen	Schreiben	networkSettings*		ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateTags ec2:DeleteNetworkInterface ec2:DeleteNetworkI

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
					nterfacePermission ec2:ModifyNetworkInterfaceAttribute
			portal*		
Associate TrustStore	Gewährt die Berechtigung zum Zuordnen von Vertrauensspeicher mit Webportalen	Schreiben	portal*		
			trustStore*		
Associate UserAccessLoggingSettings	Gewährt die Berechtigung zum Zuordnen von Benutzerzugriff-Protokollierungseinstellungen zu Webportalen	Schreiben	portal*		kinesis:PutRecord kinesis:PutRecords
			userAccessLoggingSettings*		
Associate UserSettings	Gewährt die Berechtigung zum Zuordnen von Benutzereinstellungen mit Webportalen	Schreiben	portal*		
			userSettings*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateBrowserSettings	Gewährt die Berechtigung zum Erstellen von Browsereinstellungen	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey
CreateIdentityProvider	Gewährt die Berechtigung zum Erstellen von Identitätsanbietern	Schreiben	identityProvider* portal*		
CreateIpAccessSettings	Gewährt die Berechtigung zum Erstellen von IP-Zugriffseinstellungen	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	
CreateNetworkSettings	Gewährt die Berechtigung zum Erstellen von Netzwerkeinstellungen	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreatePortal	Gewährt die Berechtigung zum Erstellen von Webportalen	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey
CreateTrustStore	Gewährt die Berechtigung zum Erstellen von Vertrauensspeichern	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	
CreateUserAccessLoggingSettings	Gewährt die Berechtigung zum Erstellen von Benutzerzugriff-Protokollierungseinstellungen	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
CreateUserSettings	Gewährt die Berechtigung zum Erstellen von Benutzereinstellungen	Schreiben		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteBrowserSettings	Gewährt die Berechtigung zum Löschen von Browsereinstellungen	Schreiben	browserSettings*		
DeleteIdentityProvider	Gewährt die Berechtigung zum Löschen von Identitätsanbietern	Schreiben	identityProvider* portal*		
DeleteIpAccessSettings	Gewährt die Berechtigung zum Löschen von IP-Zugriffseinstellungen	Schreiben	ipAccessSettings*		
DeleteNetworkSettings	Gewährt die Berechtigung zum Löschen von Netzwerkeinstellungen	Schreiben	networkSettings*		
DeletePortal	Gewährt die Berechtigung zum Löschen von Webportalen	Schreiben	portal*		
DeleteTrustStore	Gewährt die Berechtigung zum Löschen von Vertrauensspeichern	Schreiben	trustStore*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DeleteUserAccessLoggingSettings	Gewährt die Berechtigung zum Löschen von Benutzerzugriff-Protokollierungseinstellungen	Schreiben	userAccessLoggingSettings*		
DeleteUserSettings	Gewährt die Berechtigung zum Löschen von Benutzereinstellungen	Schreiben	userSettings*		
DisassociateBrowserSettings	Gewährt die Berechtigung zum Trennen der Zuordnung von Browsereinstellungen zu Webportalen	Schreiben	portal*		
DisassociateIpAccessSettings	Gewährt die Berechtigung zum Trennen der Protokollierung des IP-Zugriffs von Webportalen	Schreiben	portal*		
DisassociateNetworkSettings	Gewährt die Berechtigung zum Trennen der Zuordnung von Netzwerkeinstellungen zu Webportalen	Schreiben	portal*		
DisassociateTrustStore	Gewährt die Berechtigung zum Trennen der Zuordnung von Vertrauensspeicher mit Webportalen	Schreiben	portal*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
DisassociateUserAccessLoggingSettings	Gewährt die Berechtigung zum Trennen der Zuordnung von Benutzerzugriff-Protokollierungseinstellungen von Webportalen	Schreiben	portal*		
DisassociateUserSettings	Gewährt die Berechtigung zum Trennen der Zuordnung von Benutzereinstellungen zu Webportalen	Schreiben	portal*		
GetBrowserSettings	Gewährt die Berechtigung zum Abrufen von Details über Browsereinstellungen	Lesen	browserSettings*		
GetIdentityProvider	Gewährt die Berechtigung zum Abrufen von Details über Identitätsanbieter	Lesen	identityProvider*		
GetIpAccessSettings	Gewährt die Berechtigung zum Abrufen von Details zu IP-Zugriffseinstellungen	Lesen	ipAccessSettings*		
GetNetworkSettings	Gewährt die Berechtigung zum Abrufen von Details über Netzwerkeinstellungen	Lesen	networkSettings*		
GetPortal	Gewährt die Berechtigung zum Abrufen von Details über Webportale	Lesen	portal*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetPortalServiceProviderMetadata	Gewährt die Berechtigung zum Abrufen von Metadaten-Informationen für Serviceanbieter für Webportale	Lesen	portal*		
GetTrustStore	Gewährt die Berechtigung zum Abrufen von Details über Vertrauensspeicher	Lesen	trustStore*		
GetTrustStoreCertificate	Gewährt die Berechtigung zum Abrufen von Zertifikaten von Vertrauensspeicher	Lesen	trustStore*		
GetUserAccessLoggingSettings	Gewährt die Berechtigung zum Abrufen von Details zu den Benutzerzugriff-Protokollierungseinstellungen	Lesen	userAccessLoggingSettings*		
GetUserSettings	Gewährt die Berechtigung zum Abrufen von Details über Benutzereinstellungen	Lesen	userSettings*		
ListBrowserSettings	Gewährt die Berechtigung zum Auflisten von Browsereinstellungen	Lesen			
ListIdentityProviders	Gewährt die Berechtigung zum Auflisten von Identitätsanbietern	Lesen	identityProvider*		
ListIpAccessSettings	Gewährt die Berechtigung zum Auflisten von IP-Zugriffseinstellungen	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ListNetworkSettings	Gewährt die Berechtigung zum Auflisten von Netzwerkeinstellungen	Lesen			
ListPortals	Gewährt die Berechtigung zum Auflisten von Webportalen	Lesen			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine Ressource	Lesen			
ListTrustStoreCertificates	Gewährt die Berechtigung zum Auflisten von Zertifikaten in einem Vertrauensspeicher	Lesen			
ListTrustStores	Gewährt die Berechtigung zum Auflisten von Vertrauensspeichern	Lesen			
ListUserAccessLoggingSettings	Gewährt die Berechtigung zum Auflisten von Benutzerzugriff-Protokollierungseinstellungen	Lesen			
ListUserSettings	Gewährt die Berechtigung zum Auflisten von Benutzereinstellungen	Lesen			
TagResource	Gewährt die Berechtigung zum Hinzufügen eines oder mehrerer Tags zu einer Ressource	Markieren	browserSettings		
			ipAccessSettings		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			networkSettings		
			portal		
			trustStore		
			userAccessLoggingSettings		
			userSettings		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung, ein oder mehrere Tags aus einer Ressource zu entfernen	Markierung	browserSettings		
			ipAccessSettings		
			networkSettings		
			portal		
			trustStore		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			userAccessLoggingSettings		
			userSettings		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateBrowserSettings	Gewährt die Berechtigung zum Aktualisieren von Browsereinstellungen	Schreiben	browserSettings*		
UpdateIdentityProvider	Gewährt die Berechtigung zum Aktualisieren von Identitätsanbietern	Schreiben	identityProvider*		
			portal*		
UpdateIpAccessSettings	Gewährt die Berechtigung zum Aktualisieren von IP-Zugriffseinstellungen	Schreiben	ipAccessSettings*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateNetworkSettings	Gewährt die Berechtigung zum Aktualisieren von Netzwerkeinstellungen	Schreiben	networkSettings*		ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateTags ec2:DeleteNetworkInterface ec2:DeleteNetworkInterfacePermission ec2:ModifyNetworkInterfaceAttribute
UpdatePortal	Gewährt die Berechtigung zum Aktualisieren von Webportalen	Schreiben	portal*		
UpdateTrustStore	Gewährt die Berechtigung zum Aktualisieren von Vertrauensspeichern	Schreiben	trustStore*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
UpdateUserAccessLoggingSettings	Gewährt die Berechtigung zum Aktualisieren von Benutzerzugriff-Protokollierungseinstellungen	Schreiben	userAccessLoggingSettings*		kinesis:PutRecord kinesis:PutRecords
UpdateUserSettings	Gewährt die Berechtigung zum Aktualisieren von Benutzereinstellungen	Schreiben	userSettings*		

Von Amazon WorkSpaces Web definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
browserSettings	`arn:${Partition}:workspaces-web:${Region}:${Account}:browserSettings/${BrowserSettingsId}`	aws:ResourceTag/${TagKey}
identityProvider	`arn:${Partition}:workspaces-web:${Region}:${Account}:identityProvider/${PortalId}/${IdentityProviderId}`	

Ressourcentypen	ARN	Bedingungsschlüssel
networkSettings	`arn:${Partition}:workspaces-web:${Region}:${Account}:networkSettings/${NetworkSettingsId}`	aws:ResourceTag/${TagKey}
portal	`arn:${Partition}:workspaces-web:${Region}:${Account}:portal/${PortalId}`	aws:ResourceTag/${TagKey}
trustStore	`arn:${Partition}:workspaces-web:${Region}:${Account}:trustStore/${TrustStoreId}`	aws:ResourceTag/${TagKey}
userSettings	`arn:${Partition}:workspaces-web:${Region}:${Account}:userSettings/${UserSettingsId}`	aws:ResourceTag/${TagKey}
userAccessLoggingSettings	`arn:${Partition}:workspaces-web:${Region}:${Account}:userAccessLoggingSettings/${UserAccessLoggingSettingsId}`	aws:ResourceTag/${TagKey}
ipAccessSettings	`arn:${Partition}:workspaces-web:${Region}:${Account}:ipAccessSettings/${IpAccessSettingsId}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für Amazon WorkSpaces Web

Amazon WorkSpaces Web definiert die folgenden Bedingungsschlüssel, die im `Condition`-Element einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Aktionen, Ressourcen und Bedingungsschlüssel für AWS X-Ray

AWS X-Ray (Servicepräfix: `xray`) stellt die folgenden servicespezifischen Ressourcen, Aktionen und Bedingungskontextschlüssel für die Verwendung in IAM-Berechtigungsrichtlinien bereit.

Referenzen:

- Erfahren Sie, wie Sie diesen Service konfigurieren.
- Zeigen Sie eine Liste der API-Operationen an, die für diesen Service verfügbar sind.
- Erfahren Sie, wie Sie diesen Service und seine Ressourcen mithilfe von IAM-Berechtigungsrichtlinien schützen.

Themen

- Von AWS X-Ray definierte Aktionen
- Von AWS X-Ray definierte Ressourcentypen
- Bedingungsschlüssel für AWS X-Ray

Von AWS X-Ray definierte Aktionen

Sie können die folgenden Aktionen im Element `Action` einer IAM-Richtlinienanweisung angeben. Verwenden Sie Richtlinien, um Berechtigungen zum Ausführen einer Operation in AWS zu erteilen. Wenn Sie eine Aktion in einer Richtlinie verwenden, erlauben oder verweigern Sie in der Regel den Zugriff auf die API-Operation oder den CLI-Befehl mit demselben Namen. Dabei kann es mitunter

vorkommen, dass eine einzige Aktion den Zugriff auf mehr als eine Operation steuert. Alternativ erfordern einige Vorgänge mehrere verschiedene Aktionen.

Die Spalte Resource types (Ressourcentypen) der Aktionstabelle gibt an, ob die Aktion Berechtigungen auf Ressourcenebene unterstützt. Wenn es keinen Wert für diese Spalte gibt, müssen Sie alle Ressourcen ("*") im Element `Resource` Ihrer Richtlinienanweisung angeben. Wenn die Spalte einen Ressourcentyp enthält, können Sie einen ARN dieses Typs in einer Anweisung mit dieser Aktion angeben. Wenn für die Aktion eine oder mehrere Ressourcen erforderlich sind, muss der Aufrufer die Erlaubnis haben, die Aktion mit diesen Ressourcen zu verwenden. Erforderliche Ressourcen sind in der Tabelle mit einem Sternchen (*) gekennzeichnet. Wenn Sie den Ressourcenzugriff mit dem Element `Resource` in einer IAM-Richtlinie einschränken, müssen Sie für jeden erforderlichen Ressourcentyp einen ARN oder ein Muster angeben. Einige Aktionen unterstützen mehrere Ressourcentypen. Wenn der Ressourcentyp optional ist (nicht als erforderlich angegeben), können Sie sich für einen der optionalen Ressourcentypen entscheiden.

Die Spalte Bedingungsschlüssel der Tabelle der Aktionen enthält Schlüssel, die Sie im Element `Condition` einer Richtlinienanweisung angeben können. Weitere Informationen zu den Bedingungsschlüsseln, die den Ressourcen für den Service zugeordnet sind, finden Sie in der Spalte Bedingungsschlüssel der Tabelle der Ressourcentypen.

> **Note**
>
> Die Ressourcenbedingungsschlüssel sind in der Tabelle Ressourcentypen enthalten. Sie finden einen Link zu dem Ressourcentyp, der für eine Aktion gilt, in der Spalte Ressourcentypen (*erforderlich) der Tabelle „Aktionen“. Der Ressourcentyp in der Tabelle „Ressourcentypen“ enthält die Spalte Bedingungsschlüssel. Das sind die Ressourcenbedingungsschlüssel, die für eine Aktion in der Tabelle „Aktionen“ gelten.

Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Aktionen

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
BatchGetTraceSumma	Gewährt die Berechtigung zum Abrufen von Metadaten	Lesen			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
ryById [nur Berechtigung]	einer Liste von Ablaufverfolgungen, die anhand der ID angegeben werden				
BatchGetTraces	Gewährt die Berechtigung zum Abrufen einer Liste von Traces, die anhand der ID angegeben werden. Jede Ablaufverfolgung ist eine Sammlung von Segmentdokumenten, die von einer einzigen Anforderung stammt. Mit GetTraceSummaries können Sie eine Liste von Ablaufverfolgungs-IDs abrufen.	List			
CreateGroup	Gewährt die Berechtigung zum Erstellen einer Gruppenressource mit einem Namen und einem Filterausdruck	Write	group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSamplingRule	Gewährt die Berechtigung zum Erstellen einer Regel zur Steuerung des Samplingverhaltens für instrumentierte Anwendungen	Write	sampling-rule*		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteGroup	Gewährt die Berechtigung zum Löschen einer Gruppenressource	Schreiben	group*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	Gewährt die Berechtigung zum Löschen von Ressourcenrichtlinien	Schreiben			
DeleteSamplingRule	Gewährt die Berechtigung zum Löschen einer Samplingregel	Schreiben	sampling-rule*		
				aws:ResourceTag/${TagKey}	
GetDistinctTraceGraphs [nur Berechtigung]	Gewährt die Berechtigung zum Abrufen eines Servicediagramms für eine oder mehrere bestimmte Ablaufverfolgungs-IDs	Lesen			
GetEncryptionConfig	Gewährt die Berechtigung zum Abrufen der aktuellen Verschlüsselungskonfiguration für X-Ray-Daten	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetGroup	Gewährt die Berechtigung zum Abrufen von Gruppen-Ressourcendetails	Read	group*		
				aws:ResourceTag/${TagKey}	
GetGroups	Gewährt die Berechtigung zum Abrufen aller aktiven Gruppendetails	Read			
GetInsight	Gewährt die Berechtigung zum Abrufen der Details eines bestimmten Einblicks	Read			
GetInsightEvents	Gewährt die Berechtigung zum Abrufen der Ereignisse eines bestimmten Einblicks	Read			
GetInsightImpactGraph	Gewährt die Berechtigung zum Abrufen des Teils des Servicediagramms, der bei einem bestimmten Einblick betroffen ist	Read			
GetInsightSummaries	Gewährt die Berechtigung zum Abrufen der Zusammenfassung aller Einblicke für eine Gruppe und einen Zeitbereich mit optionalen Filtern	Read			
GetSamplingRules	Gewährt die Berechtigung zum Abrufen aller Samplingregeln	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetSamplingStatisticSummaries	Gewährt die Berechtigung zum Abrufen von Informationen über aktuelle Samplingergebnisse für alle Samplingregeln	Read			
GetSamplingTargets	Gewährt die Berechtigung zum Anfordern einer Samplingquote für Regeln, die der Service für das Sampling von Anforderungen verwendet	Read			
GetServiceGraph	Gewährt die Berechtigung zum Abrufen eines Dokuments, das Services zur Verarbeitung eingehender Anforderungen beschreibt sowie infolgedessen aufgerufene Downstream-Services.	Read			
GetTimeSeriesServiceStatistics	Gewährt die Berechtigung, eine Zusammenfassung der Servicestatistiken abzurufen, die durch einen bestimmten Zeitraum definiert sind, der in Zeitintervallen untGewährt ist.	Read			
GetTraceGraph	Gewährt die Berechtigung zum Abrufen eines Servicediagramms für eine oder mehrere bestimmte Trace-IDs	Read			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
GetTraceSummaries	Gewährt die Berechtigung, IDs und Metadaten für Ablaufverfolgungen, die für einen bestimmten Zeitraum verfügbar sind, mithilfe eines optionalen Filters abzurufen. Um die vollständigen Ablaufverfolgungen abzurufen, übergeben Sie die Ablaufverfolgungs-IDs an BatchGetTraces.	Lesen			
Link [nur Berechtigung]	Gewährt die Berechtigung zum Freigeben von X-Ray-Ressourcen für ein Überwachungs-Konto	Schreiben			
ListResourcePolicies	Gewährt die Berechtigung zum Auflisten von Ressourcenrichtlinien	Auflisten			
ListTagsForResource	Gewährt die Berechtigung zum Auflisten von Tags für eine X-Ray-Ressource	List	group		
			sampling-rule		
PutEncryptionConfig	Gewährt die Berechtigung zum Aktualisieren der Verschlüsselungskonfiguration für X-Ray-Daten	Berechtigungsverwaltung			

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
PutResourcePolicy	Gewährt die Berechtigung zum Erstellen oder Aktualisieren von Ressourcenrichtlinien	Schreiben			
PutTelemetryRecords	Gewährt die Berechtigung, AWS X-Ray-Daemon-Telemetrie an den Service zu senden	Write			
PutTraceSegments	Gewährt die Berechtigung zum Upload von Segmentdokumenten in AWS X-Ray. Das X-Ray-SDK generiert Segmentdokumente und sendet diese an den X-Ray-Daemon, der sie in Batches hochlädt.	Write			
TagResource	Gewährt die Berechtigung zum Hinzufügen von Tags zu einer X-Ray-Ressource	Markieren	group		
			sampling-rule		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Gewährt die Berechtigung zum Entfernen von Tags aus einer X-Ray-Ressource	Markieren	group		

Aktionen	Beschreibung	Zugriffsebene	Ressourcentypen (*erforderlich)	Bedingungsschlüssel	Abhängige Aktionen
			sampling-rule		
				aws:TagKeys	
UpdateGroup	Gewährt die Berechtigung zum Aktualisieren einer Gruppenressource	Write	group*		
				aws:ResourceTag/${TagKey}	
UpdateSamplingRule	Gewährt die Berechtigung zum Ändern der Konfiguration einer Samplingregel	Write	sampling-rule*		
				aws:ResourceTag/${TagKey}	

Von AWS X-Ray definierte Ressourcentypen

Die folgenden Ressourcentypen werden von diesem Service definiert und können im Element `Resource` von IAM-Berechtigungsrichtlinienanweisungen verwendet werden. Jede Aktion in der Tabelle "Actions" (Aktionen) identifiziert die Ressourcentypen, die mit der Aktion angegeben werden können. Ein Ressourcentyp kann auch definieren, welche Bedingungsschlüssel Sie in einer Richtlinie einschließen können. Diese Schlüssel werden in der letzten Spalte der Tabelle der Ressourcentypen angezeigt. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Resource types.

Ressourcentypen	ARN	Bedingungsschlüssel
group	`arn:${Partition}:xray:${Region}:${Account}:group/${GroupName}/${Id}`	aws:ResourceTag/${TagKey}
sampling-rule	`arn:${Partition}:xray:${Region}:${Account}:sampling-rule/${SamplingRuleName}`	aws:ResourceTag/${TagKey}

Bedingungsschlüssel für AWS X-Ray

AWS X-Ray definiert die folgenden Bedingungsschlüssel, die im Element `Condition` einer IAM-Richtlinie verwendet werden können. Diese Schlüssel können Sie verwenden, um die Bedingungen zu verfeinern, unter denen die Richtlinienanweisung angewendet wird. Details zu den Spalten in der folgenden Tabelle finden Sie in der Tabelle Condition keys (Bedingungsschlüssel).

Eine Liste der globalen Bedingungsschlüssel, die für alle Services verfügbar sind, finden Sie unter Verfügbare globale Bedingungsschlüssel.

Bedingungsschlüssel	Beschreibung	Typ
aws:RequestTag/${TagKey}	Filtert den Zugriff durch die Tags, die in der Anfrage übergeben werden	Zeichenfolge
aws:ResourceTag/${TagKey}	Filtert den Zugriff basierend auf den Tags, die der Ressource zugeordnet sind.	Zeichenfolge
aws:TagKeys	Filtert den Zugriff basierend auf den Tag-Schlüssel, die in der Anfrage übergeben werden	ArrayOfString

Zugehörige Ressourcen

Weitere Informationen aus dem Leitfaden IAM-Benutzerhandbuch finden Sie in folgenden verwandten Ressourcen:

- Praktische Anleitung: Erstellen und Anfügen Ihrer ersten vom Kunden verwalteten Richtlinie
- AWS Services, die mit IAM arbeiten
- Auswertungslogik für Richtlinien

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.